POLYCOM®

Polycom RMX™ 2000/4000 Release Notes for Maximum Security Environments

Version 5.1.0.G | December 2010 | DOC2573A

Trademark Information

Polycom®, the Polycom "Triangles" logo, and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common-law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

Patent Information

The accompanying product is protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

© 2010 Polycom, Inc. All rights reserved.

Polycom, Inc.
4750 Willow Road
Pleasanton, CA 94588-2708
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

Table of Contents

New Hardware - RMX 4000 1
Version 5.1.0.G - New Features List 2
Version 5.1.0.G - Changes to Existing Features 3
Version 4.5.0.F - Features List (Enhanced Security Mode) 5
Version 5.1.0.G - Upgrade Package Contents 8
Where to Get the Latest Product Information 8
Version 5.1.0.G - Interoperability Tables 9
Devices 9
RMX Web Client 11
Unsupported Features 11
Version 5.1.0.G - Upgrade Procedure 12
Upgrade Paths to Version 5.1.0.G 12
Upgrading from Version 4.5.0.F to Version 5.1.0.G (RMX 2000) 12
Upgrading from Version 5.0.2 to Version 5.1.0.G 14
Upgrading to Version 5.0.2 15
Upgrading from Version 5.0/5.0.1 to Version 5.0.2 15
Upgrading from Version 3.x/4.x to Version 5.0.2 16
IVR Services Update 18
RMX Manager Upgrade 18
Detailed Description - Polycom RMX™ 4000 19
Hardware Additions 19
System Capacities 20
Resource Capacities 21
Redundancy 21
Network Separation 22
Hardware Monitor Changes 22
Component Slot Allocation 22
Hardware Monitor UI Changes 23
RMX 4000 Properties 24
CNTL4000 Properties 24
FSM (Fabric Switch Module) 4000 Properties 25
Backplane 4000 Properties 25
RTM IP4000 Properties 25
LAN Unit List Properties 26
RTM LAN Properties 26
Fans Properties 26
Hardware Monitor Diagnostic Changes 27
Video/Voice Port Configuration Changes 28
Resource Report Changes 28
RMX 4000 Banner 29
Network Service Changes 29
Fast Configuration Wizard Change 29
Management Network Change 30
IP Service Change 30
Ethernet Settings 30

Version 5.1.0.G Detailed Description 32
Audible Alarms 32
Using Audible Alarms 32
Audible Alarm Permissions 32
Stop Repeating Message 32
Configuring the Audible Alarms 33
User Customization 33
Replacing the Audible Alarm File 34
Recording Link Encryption 35
SIP Dial-in Busy Notification 37
Version 4.5.0.F Detailed Description - General 38
IPv6 Support 38
IPv6 Networking Addresses for RMX Internal and External Entities 38
RMX Internal Addresses 38
External Entities 38
IPv6 Guidelines 38
Using IPv6 Addressing 39
Management Network Service 39
Default IP Network Service 44
Fast Configuration Wizard 44
IP Network Monitoring 52
H.320 Encryption 56
Media Encryption Guidelines 56
Ping RMX 58
Guidelines 58
Using Ping 58
Version 4.5.0.F Detailed Description - Security Enhancements 59
Enhanced Security Mode (JITC_MODE) 59
JITC_MODE System Flag 59
Force Secured Communications Mode 61
Restricted File Uploading 62
Network Security 62
Signaling and Management Network Separation 62
Banner Display and Customization 63
Customizing Banners 63
Banner Display 64
Login Screen Banner 64
Main Screen Banner 65
Users Management 66
Managing the RMX Users 66
User Types 66
Disabling/Enabling Users 66
Renaming Users 66
Disabling Inactive Users 67
Managing the User Login Process 67
Implementing Password Re-Use / History Rules 68
Defining Password Aging 68
Defining Password Change Frequency 69
Forcing Password Change 69
Managing Conference and Chairperson Passwords 69

Temporary User Lockout 70
User Lockout 70
User Login Record 70
Controlling RMX User Sessions 71
Management Sessions per System 71
Sessions per User 71
Connection Timeout 71
Session Timeout 71
Erase Session History After Logout 71
Cyclic File System Alarm 72
Cyclic Files 72
Restricting Content Broadcast to Lecturer 73
Version 4.5.0.F Detailed Description - Changes to Existing Features..... 74
User Management 74
Disabling, Enabling and Renaming Users 74
Disabling a User 74
Enabling a User 74
Renaming a User 75
Software Management 76
System Backup and Restore 76
Backup and Restore Guidelines 76
Installing RMX Manager for Secure Communication Mode 77
Using an Internal Certificate Authority 80
Additional Auditor Features and Events 84
Dial-out Extension/Identifier String 85
New CDR Events 86
New Active Alarms 87
Corrections and Known Limitations..... 89
Corrections Between Version 4.5.0.F and Version 5.1.0.G 89
Corrections Between Version 4.1.1 and Version 5.0 94
Version 5.1.0.G System Limitations 96

New Hardware - RMX 4000

A new MCU has been added to the RMX range of MCUs. It has the key features of the *RMX 2000* with the following additions/changes:

Table 1 *RMX 4000 Additions and Changes*

	Feature Name	Description
1	New and modified cards	New cards and modified components have been added to the Hardware.
2	System Capacity	Number of MPM+ media cards that can be installed on the system has increased from 2 to 4. The change in resources and the number of cards is reflected in the: • Network Services • Video/Voice Port Configuration • Resource Report
3	Redundancy	The RMX 4000 has a number of built in redundant components: • Redundant AC power supply, hot swappable • Redundant DC power supply • Fans (8 units), a Field Replaceable Unit (FRU)
4	Network Separation	The RMX 4000 provides enhanced security by physically separating the Media, Signaling and Management networks from each other. The Signaling network, Management network and each of the media cards has its own network connection. All MPM+ cards must have IP addresses on the same network as the signaling network.
5	RMX Type Indication	RMX Banner and Welcome heading display the RMX Type accordingly.
6	Hardware Monitor	New and dedicated slots. New card properties.

Version 5.1.0.G - New Features List

The following table lists the new features in *Version 5.1.0.G* (*RMX 2000* and *RMX 4000*).

Table 2 *New Features List - RMX 2000 and RMX 4000*

	Category	Feature Name	Description
1	General	Audible Alarms	Previously, the RMX users had to rely on visual cues to detect events occurring on the RMX. In *Version 5.1.0.G*, in addition to the visual cues, an audible alarm can be activated and played when participants request Operator Assistance.

Version 5.1.0.G - Changes to Existing Features

The following table lists the changes to existing features in Version 5.1.0.G.

Table 3 *Feature Changes List*

	Category	Feature Name	Description
1	General	Operating System	Linux 2.6.33.4 is installed as RMX operating system during upgrade. **Note:** In systems with MPM cards only, Linux 2.4 is installed as the Operating system.
2	General	Active Alarms	New Active Alarms were added.
3	General	Dial-out Participant Properties	The new Extension/Identifier field was added to the Participant Properties to enable to add the extension or conference password to the dialing string.
4	General	System flag - Site Names	The display of site names can be cancelled by changing the default setting of the **HIDE_SITE_NAMES** system flag from OFF (default) to **ON**. When set to ON, the flag SITE_NAMES_ALWAYS_ON is ignored.
5	General	System flag - Ad-hoc Conference Duration	The duration of ad-hoc conference* can be configured on a system level by setting the **CHANGE_AD_HOC_CONF_DURATION** system flag to one of the following values (in minutes): **60** (default), **90**, **180** and **270**. * An ad-hoc conference is automatically created when the participant dials into an Ad-hoc Entry Queue and enters a conference ID that is not being used by any other conferencing entity. It is based on the Conference Profile assigned to the EQ.
6	General	Recording	The Recording Link can be encrypted when recording an encrypted conference. The encryption of the *Recording Link* is enabled when *Encryption* is selected in the *Conference Profile* on the RMX and on the RSS, and the system flag ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF is set to NO (default). **Note:** When the JITC_MODE flag is set to YES, this feature is not supported.
7	General	RMX 2000 System capacity	Maximum number of video participants in a single conference increased from 80 to 160 on the RMX 2000.

Table 3 *Feature Changes List*

	Category	Feature Name	Description
8	General/IP	System configuration - SIP Dial in	When the new system flag SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD is set to YES (NO is the default), it enables the RMX to send a busy notification to a SIP audio endpoint or a SIP device when dialing in to the RMX whose audio resource usage exceeded the Port Usage threshold.
9	IP	LPR	Previously, when packet loss was detected on a network, the LPR/DBA mechanism gradually decreased the conference's Line Rate until packet loss was no longer detected. Once decreased, the line rate never increased back to the conference's Line Rate when network packet loss was no longer detected. In version 5.0.1, the mechanism has been changed so that when packet loss is no longer detected, the DBA gradually increases the line rate until the initial conference Line Rate settings are reached. If packet loss re-occurs the LPR/DBA mechanism decreases the Line Rate and the cycle is repeated. If the Line Rate returns to the initial conference Line Rate, the LPR/DBA mechanism is automatically inactive.
10	Diagnostics	New Components added to diagnostics	In RMX 2000, RTM IP and RTM ISDN components are included in the diagnostic tests.
11	Diagnostics	RMX 4000 components	The logical components of RMX 4000 that are similar to RMX 2000 are included in the diagnostic tests.

Version 4.5.0.F - Features List (Enhanced Security Mode)

The following table lists the enhanced security features in Version 4.5.0.F (RMX 2000).

Table 4 *New Features List - RMX 2000 and RMX 4000 (Continued)*

	Category	Feature Name	Description
General			
1	IP	IPv6 Support	IPv6 Addressing is supported. **Note:** This option is implemented in RMX 2000 systems with MPM+ cards only.
2	ISDN	Encryption	H.320 Encryption is supported. **Note:** This option is implemented in RMX 2000 systems with MPM+ cards only.
3	General	Login screen and main screen Banners	General information or Warning banners can be added to the Login Screen and the Main Screen display.
4	General	Ping	The *Ping* administration tool enables the RMX Signaling Host to test network connectivity by *Pinging* IP addresses.
5	General	Operating System	Linux 2.6.24 is installed as RMX operating system during upgrade. **Note:** In systems with MPM cards only, Linux 2.4 is installed as the Operating system.
6	General	RMX Manager	Installation of RMX Manager for use with an RMX that is in Secure Communication Mode.
7	General	CDR	New events were added to the CDR: • RESERVED_PARTICIPANT_CONTINUE_IPV6_ADDRESS (2011) • USER_ADD_PARTICIPANT_CONTINUE_IPV6_ADDRESS (2102) • USER_UPDATE_PARTICIPANT_CONTINUE_IPV6_ADDRESS (2106) • EVENT_NEW_UNDEFINED_PARTY_CONTINUE_IPV6_ADDRESS (32) Each of this events contain the IPv6 address of the participant's endpoint.

Table 4 *New Features List - RMX 2000 and RMX 4000 (Continued)*

	Category	Feature Name	Description
Enhanced Security Features			
8	General	Enhanced Security Mode (JITC_MODE)	The RMX can operate in one of two modes: standard mode (Non-JITC Mode) or Enhanced Security Mode (JITC Mode). In the Enhanced Security Mode the enhanced security features of the version are rigorously enforced.
9	IP Network	Network Separation **(RMX 2000 with MPM+ Cards only, and the Enhanced Security Mode is enabled)**	Network security can be enhanced by separation of the Signaling and Management Networks. When network separation is enabled, signaling between IP endpoints and the RMX is via the LAN 2 port, while all RMX management sessions are hosted via the LAN 3 port. LAN2 and LAN3 IP addresses can be on separate networks. **Note:** Network Separation can be implemented only in RMX systems that include MPM+ cards only and the system flag JITC_MODE is set to YES.
10	User Management	RMX Users	Managing RMX users includes: • User types that are not supported when the Enhanced Security environment is enabled. • Disabling and enabling RMX Users • Renaming RMX Users • Disabling inactive users
11	User Management	Login Password Process	Managing the user login process includes: • Implementing Strong Passwords • Implementing password re-use / history rules • Defining password aging rules • Defining password change frequency • Forcing password change • Conference and Chairman Password management • Locking out Users • Displaying the User Login record

Table 4 *New Features List - RMX 2000 and RMX 4000 (Continued)*

	Category	Feature Name	Description
12	User Management	User Sessions	Controlling the User Sessions includes: • Limiting the maximum number of concurrent user sessions (http/https connections) • Connection Timeout • User session timeout • Limiting the maximum number of users that can connect to the system (number of concurrent http/https connections)
13	General	Cyclic File System Alarm	The system flag ENABLE_CYCLIC_FILE_SYSTEM _ALARMS enables the system to display active alarms when logger/CDR/fault files may be overwritten due to automatic backup, deletion and restoring of files in Cyclic mode.
14	General	FIPS 140-2 Compliance	A certified FIPS library is used to ensure that all Cryptographic Modules are compliant with Federal Information Processing Standard - FIPS 140-2. All passwords are encrypted.

Version 5.1.0.G - Upgrade Package Contents

The JITC Version package must be downloaded from the *Polycom Resource Center* and includes the following items:

- lan.cfg file
- LanConfigUtility.exe
- RMX Documentation
  - Polycom RMX 2000/4000 System Release Notes for Maximum Security environments
  - Polycom RMX 2000/4000 Deployment Guide for Maximum Security environments
  - Polycom RMX 2000/4000 System Administrator's Guide for Maximum Security environments
  - RMX 2000 Hardware Guide
  - RMX 4000 Hardware Guide
  - RMX Third Party Licenses
- External DB Tools *Version 4.0*
  - RMX 2000 External Database API Programmer's Guide
  - Sample Scripts
- RMX XML API Kit *Version 5.0*
  - RMX 2000/4000 XML API *Version 5.0* Release Notes
  - RMX 2000/4000 XML API Overview
  - RMX 2000/4000 XML API Schema Reference Guide (*Version 5.0*)
  - MGC to RMX XML API Conferencing Comparison
  - Polycom XML Tracer User's Guide
  - XML Schemas
  - Polycom XML Tracer application

Where to Get the Latest Product Information

To view the latest Polycom product documentation, visit the **Support** section of the Polycom website at ***www.polycom.com/support***.

Version 5.1.0.G - Interoperability Tables

Devices

The following table lists the devices and versions with which RMX *Version 5.1.0.G* was tested. Supported versions include also previous versions.

Table 5 *Version 5.1.0.G Device Interoperability Table*

Device	Version
Gatekeepers/Proxies	
Polycom CMA	4.01.04.ER011/ 4.01.05 Beta Code
Polycom PathNavigator	7.0.12
Polycom SE200	3.00.07.ER001
Cisco gatekeeper	12.3
Radvision ECS gatekeeper	3.5.2.5
Iptel proxy	0.9.6
Microsoft OCS	R1 / R2
Recorder	
Polycom RSS 2000	4.0.0.001 360
Polycom RSS 4000	4.0 and 5.0
MCUs and Call Managers	
Polycom MGC 25/50/100 and MGC+50/100	8.0.2 and 9.0.3
RMX 1000	2.1
Polycom DMA 7000	1.1.1/2.0.0 Beta
Avaya CM	5.2
Avaya ACM	943
Avaya IP Softphone R6.0	SP1
Cisco Call Manager	4.1
Tandberg MCU	D3.11
Tandberg MPS	J3.3
Endpoints	
Polycom HDX Family	2.5.0.6 / 2.5.0.7 Beta
Polycom VSX product line	9.0.5.1

Table 5 *Version 5.1.0.G Device Interoperability Table (Continued)*

Device	Version
Polycom Viewstation	7.5.4
Polycom CMAD	4.1.1.1010 / 4.1.2.0.178
Polycom QDX6000	4.0
Polycom VVX1500	3.2.2.0191
Polycom ViaVideo PVX	8.0.4
Polycom VS 512	7.5.4
Polycom VSSP 128/384	7.5.4
Polycom VS EX	6.0.5
Polycom VS 4000	6.0.5
Polycom VS FX	6.0.5
Polycom V700 and Polycom V500	9.0.5.1
Polycom iPower 9000	6.2.1208
Soundstation IP3000	2.8
Aethra X3	11.3.23
Aethra X7	12.1.7
Aethra VegaStar Gold	6.0.49
Avaya IP Softphone R6	6.01.48
Avaya 1XC	R1.020-SP2-1696
LifeSize	4.2.0.17
LifeSize Room and Express	4.2.0.17
VVX1500	3.1.2.0256
DST B5	2.0
DST K60	2.0.1
DST K80	4.0
Sony PCS -XG80	2.0.4
Sony PCS -1	3.42
Sony PCS -G50	2.70
Sony PCS -TL50	2.42
Tandberg 150 MXP	F8.1
Tandberg MXP Product line	F8.1
Tandberg Classic E-Series	E5.3 PAL
Tandberg 880 E	F8.1
Microsoft OC client R2	3.5.6907.37

Nortel environment is supported only with RMX 2.0.2 Nortel designated version. *Version 2.0.2* is only supported on RMX A/B/C- type chassis with MPM cards only and no MPM+ cards.

RMX Web Client

The following table lists the environments (Web Browsers and Operating Systems) with which the *RMX Web Client* was tested.

Table 6 *Version 5.0 Environment Interoperability Table*

Web Browser	Operating System
Internet Explorer 6	Windows XP™
Internet Explorer 7	Windows XP™
	Windows Vista™

Unsupported Features

When the **JITC_MODE** flag is set to **YES,** *Version 5.1.0.G* does not include support for:

- Connection to Alternate Management Network via LAN3 port
- SUPPORT user
- Auditor user
- Chairperson user
- Connections to External Databases
- IP Sec security protocols
- ISDN Cascade
- Serial connection
- Modem connection
- MPM cards
- NTP
- QoS with IPv6
- Recording link
- SIP security (Digest)
- SIP TLS
- SNMP
- SSH server.
- USB key configuration
- Web link (Hyperlink in Participant Properties dialog box)

Version 5.1.0.G - Upgrade Procedure

Upgrade Paths to Version 5.1.0.G

The upgrade paths to *Version 5.1.0.G* from both the previous *Maximum Security* version and previous standard versions are summarized in Table 7.

When upgrading from *Version 2.x*, the upgrades to both the first and second intermediate versions must be performed.

Table 7 *Upgrade Paths to Version 5.1.0.G*

Current Version	First Intermediate Upgrade		Second Intermediate Upgrade		New Version	
	Version	Key	Version	Key	Version	Key
4.5.0.F	N/A		N/A		**5.1.0.G**	Yes
5.0.x	5.0.2	No	N/A		**5.1.0.G**	Yes
3.x / 4.x	5.0.2	Yes	N/A		**5.1.0.G**	Yes
2.x	4.1.1	Yes	5.0.2	Yes	**5.1.0.G**	Yes

Upgrading from Version 4.5.0.F to Version 5.1.0.G (RMX 2000)

When upgrading from *Version 4.5.0.F*, it is essential that you upgrade directly to *Version 5.1.0.G*. Do not perform any intermediate upgrade

1. Download the required software *Version 5.1.0.G* from the *Polycom Resource Center* web site.
2. Obtain the *Version 5.1.0.G Product Activation Key* from the *Polycom Resource Center* web site. For more information, see the *RMX 2000/4000 Deployment Guide for Maximum Security Environments*, "*Procedure 3: First Entry Configuration*" on page **1-13**.
3. Backup the configuration file. For more information, see the *RMX 2000/4000 Deployment Guide for Maximum Security Environments*, "*System Backup and Restore*" on page **14-78**.
4. Install MCU Software *Version 5.1.0.G*.
   On the *RMX* menu, click **Administration> Software Management > Software Download**.
5. *Browse* to the *Install Path*, selecting the **Version 5.1.0.Gxx.bin** file in the folder where Version 5.1.G is saved and click **Install**.

   At the end of the installation process the system displays an indication that the software was successfully downloaded and that a new activation key is required.

6 Click **Close** to close the *Install Software* dialog box.

7 Click **Setup>Product Activation**.
The *Product Activation* dialog box is displayed with the serial number field completed.

8 In the *Activation Key* field, enter or paste the *Product Activation Key* obtained earlier and click **OK**.

9 When prompted whether to reset the MCU, click **Yes** to reset the MCU.

At the end of the installation process the system displays an indication that the software was successfully downloaded.

The upgrade procedure takes about **30** minutes during which time an *Active Alarm - System Upgrade* is displayed.

The RMX resets itself during the upgrade process and connection to the *RMX Web Client* may be lost. If the workstation is logged in to the *RMX Web Client* during the resets, the *MCU State* indicator at the bottom right corner of the *RMX Web Client* screen indicates *STARTUP.*

Sometimes when upgrading from *Version 4.5.0.F* to *Version 5.1.0.G* the reset process fails. In such a case, you can try to connect to the MCU via the Shelf Management and reset the MCU from the Hardware Monitor or you can "hard" reset the MCU by turning the Power off and on again.

10 After about **30** minutes, **close and reopen the browser** and connect to the RMX. If the browser was not closed and reopened, the following error message is displayed: "Browser environment error. Please reopen the browser".

The version number in the *Welcome* screen has changed to *5.1.0.G*

11 In the *RMX Web Client – Welcome* screen, enter your *Username* and *Password* and click **Login**.

RMX 2000

- If upgrading from Version *4.5.0.F*, after software installation, the MCU is in the last *Card Configuration Mode* that was set for the system before the software upgrade. For more information on the Card Configuration Modes, see the RMX 2000 Hardware Guide, "*MPM/ MPM+ and MPMx Media Cards"* on page **1-16**.
- If upgrading from *Version 2.x or 3.x*, after software installation, the MCU is in **MPM** *Card Configuration Mode*. For details on upgrading to MPM+, see the *RMX 2000 MPM to MPM+ Migration Procedure* document.

In the *Main Screen* an *MCU State* indicator displays a progress indicator Starting up (15:25) showing the time remaining until the system start-up is complete.

If the default POLYCOM user is defined in the RMX Web Client, an Active Alarm is created and the MCU status changes to MAJOR until the POLYCOM User is renamed or a new Administrator User is created and the default User is deleted.

An Active Alarm is created stating the Gateway Profile was not added. If Gateway funtionality is required, the Gateway Profile should be reconfigured.

To maximize conferencing performance, especially in high bit rate call environments, a 1 Gb connection is recommended for each LAN connection.

To use the new features such as *Operator Assistance* and *Gateway Sessions* the IVR Services must be updated. For more details, see "*IVR Services Update*" on page **18**.

If the upgrade process fails, please contact Polycom support.

Upgrading from Version 5.0.2 to Version 5.1.0.G

To upgrade from *Version 5.x* to Version 5.1.0.G, you must first upgrade to *Version 5.0.2* and then upgrade to *Version 5.1.0.G*. See "*Upgrading to Version 5.0.2*" on page **15**.

1. Download the required software *Version 5.1.0.G* from the *Polycom Resource Center* web site.
2. Backup the configuration file. For more information, see the *RMX 2000/4000 Administrator's Guide for Maximum Security environments*, "*System Backup and Restore*" on page **14-78**.
3. Install MCU Software *Version 5.1.0.G*.
   On the *RMX* menu, click **Administration> Software Management > Software Download**.
4. *Browse* to the *Install Path,* selecting the **Version 5.1.0.Gxx.bin** file in the folder where *Version 5.1.G* is saved and click **Install**.

   At the end of the installation process the system displays an indication that the software was successfully downloaded and that a new activation key is required.
5. Click **Close** to close the *Install Software* dialog box.
6. Click **Setup>Product Activation**.
   The *Product Activation* dialog box is displayed with the serial number field completed.
7. When prompted whether to reset the MCU, click **Yes** to reset the MCU.

   At the end of the installation process the system displays an indication that the software was successfully downloaded.

   The upgrade procedure takes about **30** minutes during which time an *Active Alarm - System Upgrade* is displayed.

   The RMX resets itself during the upgrade process and connection to the *RMX Web Client* may be lost. If the workstation is logged in to the *RMX Web Client* during the resets, the *MCU State* indicator at the bottom right corner of the *RMX Web Client* screen indicates *STARTUP.*
8. After about **30** minutes, **close and reopen the browser** and connect to the RMX.
   If the browser was not closed and reopened, the following error message is displayed: "Browser environment error. Please reopen the browser".

The version number in the *Welcome* screen has changed to *5.1.0.G*

9 In the *RMX Web Client – Welcome* screen, enter your *Username* and *Password* and click **Login**.

In the *Main Screen* an *MCU State* indicator displays a progress indicator Starting up (15:25) showing the time remaining until the system start-up is complete.

If the default POLYCOM user is defined in the RMX Web Client, an Active Alarm is created and the MCU status changes to MAJOR until a new Administrator user is created and the default user is deleted.

RMX 4000: An Active Alarm is created stating that not all RTM LAN cards have been recognized. System functionality is not affected. The Active Alarm is cleared when the system is reset.

To maximize conferencing performance, especially in high bit rate call environments, a 1 Gb connection is recommended for each LAN connection.

Upgrading to Version 5.0.2

To upgrade from *Version 2.x* to *Version 5.0.2*, you must first upgrade to *Version 4.1.1* and then upgrade to *Version 5.0.2*. If after the installation of *Version 4.1.1* the MCU reset fails, turn the system power off and on again.

Upgrading from Version 5.0/5.0.1 to Version 5.0.2

1 Download the required software *Version 5.0.2* from the *Polycom Resource Center* web site.

2 Backup the configuration file. For more information, see the *RMX Administrator's Guide for Maximum Security Environments, "System Backup and Restore"* on page 14-78.

3 Install MCU Software *Version 5.0.2*.
On the *RMX* menu, click **Administration> Software Management > Software Download**.

4 *Browse* to the *Install Path,* selecting the **Version 5.0.2xx.bin** file in the folder where *Version 5.0.2* is saved and click **Install**.

At the end of the installation process the system displays an indication that the software was successfully downloaded and that a new activation key is required.

5 Click **Close** to close the *Install Software* dialog box.

6 When prompted whether to reset the MCU, click **Yes** to reset the MCU.

At the end of the installation process the system displays an indication that the software was successfully downloaded.

The upgrade procedure takes about **30** minutes during which time an *Active Alarm - System Upgrade* is displayed.

The RMX resets itself during the upgrade process and connection to the *RMX Web Client* may be lost. If the workstation is logged in to the *RMX Web Client* during the resets, the *MCU State* indicator at the bottom right corner of the *RMX Web Client* screen indicates *STARTUP.*

7 After about **30** minutes, **close and reopen the browser** and connect to the RMX. If the browser was not closed and reopened, the following error message is displayed: "Browser environment error. Please reopen the browser".

The version number in the *Welcome* screen has changed to *5.0.2*.

8 In the *RMX Web Client – Welcome* screen, enter your *Username* and *Password* and click **Login**.

In the *Main Screen* an *MCU State* indicator displays a progress indicator Starting up (15:25) showing the time remaining until the system start-up is complete.

If the default POLYCOM user is defined in the RMX Web Client, an Active Alarm is created and the MCU status changes to MAJOR until a new Administrator user is created and the default user is deleted.

To maximize conferencing performance, especially in high bit rate call environments, a 1 Gb connection is recommended for each LAN connection.

Upgrading from Version 3.x/4.x to Version 5.0.2

When upgrading from *Version 3.x* and *4.x*, it is essential that you upgrade directly to *Version 5.0.2*. Do not perform any intermediate upgrade

1 Download the required software *Version 5.0.2* from the *Polycom Resource Center* web site.

2 Obtain the *Version 5.0.2 Product Activation Key* from the *Polycom Resource Center* web site. For more information, see the *RMX Getting Stated Guide*, *"Procedure 1: First-time Power-up"* on page **2-18**.

3 Backup the configuration file. For more information, see the *RMX Administrator's Guide for Maximum Security Environments*, *"System Backup and Restore"* on page **14-78**.

4 Install MCU Software *Version 5.0.2*.
On the *RMX* menu, click **Administration> Software Management > Software Download**.

5 *Browse* to the *Install Path,* selecting the **Version 5.0.2xx.bin** file in the folder where *Version 5.0.2* is saved and click **Install**.

At the end of the installation process the system displays an indication that the software was successfully downloaded and that a new activation key is required.

6 Click **Close** to close the *Install Software* dialog box.

7 Click **Setup>Product Activation**.
The *Product Activation* dialog box is displayed with the serial number field completed.

8 In the *Activation Key* field, enter or paste the *Product Activation Key* obtained earlier and click **OK**.

9 When prompted whether to reset the MCU, click **Yes** to reset the MCU.

At the end of the installation process the system displays an indication that the software was successfully downloaded.

The upgrade procedure takes about **30** minutes during which time an *Active Alarm - System Upgrade* is displayed.

The RMX resets itself during the upgrade process and connection to the *RMX Web Client* may be lost. If the workstation is logged in to the *RMX Web Client* during the resets, the *MCU State* indicator at the bottom right corner of the *RMX Web Client* screen indicates *STARTUP.*

Sometimes when upgrading from *Version 4.x* to *Version 5.0.x* the reset process fails. In such a case, you can try to connect to the MCU via the Shelf Management and reset the MCU from the Hardware Monitor or you can “hard” reset the MCU by turning the Power off and on again.

10 After about **30** minutes, **close and reopen the browser** and connect to the RMX. If the browser was not closed and reopened, the following error message is displayed: “Browser environment error. Please reopen the browser”.

The version number in the *Welcome* screen has changed to *5.0.2*.

11 In the *RMX Web Client – Welcome* screen, enter your *Username* and *Password* and click **Login**.

- If upgrading from *Version 4.x*, after software installation, the MCU is in the last *Card Configuration Mode* that was set for the system before the software upgrade. For more information on the Card Configuration Modes, see the RMX 2000 Hardware Guide, "*MPM/MPM+ and MPMx Media Cards”* on page **1-16**.
- If upgrading from *Version 2.x* or *3.x*, after software installation, the MCU is in **MPM** *Card Configuration Mode.* For details on upgrading to MPM+, see the *RMX 2000 MPM to MPM+ Migration Procedure* document.

In the *Main Screen* an *MCU State* indicator displays a progress indicator

showing the time remaining until the system start-up is complete.

If the default POLYCOM user is defined in the RMX Web Client, an Active Alarm is created and the MCU status changes to MAJOR until the POLYCOM User is renamed or a new Administrator User is created and the default User is deleted.

To maximize conferencing performance, especially in high bit rate call environments, a 1 Gb connection is recommended for each LAN connection.

12 To use the new features such as *Operator Assistance* and *Gateway Sessions* the IVR Services must be updated. For more details, see "*IVR Services Update*" on page **18**.

If the upgrade process fails, please contact Polycom support.

IVR Services Update

When upgrading from *Version 4.5.0.F* and earlier, Operator Assistance and the Gateway calls options require that the IVR Service includes specific (new) DTMF Codes and voice messages that are not automatically added to existing IVR Services in order to avoid conflicts with existing DTMF codes. Therefore, to use these options, new Conference and Entry Queue IVR Services must be created.

For details on modifying the IVR Services, see *RMX 2000/4000 Administrator's Guide for Maximum Security Environments*, "*Defining a New Conference IVR Service*" on page **12-9**.

RMX Manager Upgrade

When upgrading the RMX Manager from *Version 5.0.x* to *Version 5.1.0.G* you must first uninstall the RMX Manager application using **Control Panel > Add or Remove Programs** and then install the RMX Manager application as a new installation.

When upgrading the RMX Manager from *Version 4.5.0.F* to *Version 5.1.0.G*, the RMX Manager application can be installed in addition to Version 4.x installation. However, it is recommended to uninstall earlier versions of the RMX Manager and re-install the new version.

For a new RMX installation, you must first complete the RMX Installation and First Entry Configuration before installing the RMX Manager application. Once the connection to the RMX unit is established and the Login window is displayed, the RMX Manager application can be installed. For more details, see the *RMX 2000/4000 Deployment Guide for Maximum Security Environments*, "*Installing RMX Manager for Secure Communication Mode*" on page **3-1**.

For more information on the RMX Manager, see "*Audible Alarms*" on page **32**.

Detailed Description - Polycom RMX™ 4000

The Polycom RMX™ 4000 real-time media conference platform is based on advanced architecture and offers a flexible, scalable, and future-proof platform.

It natively supports multiple network types - IP (H.323, SIP), PSTN, and ISDN - to extend the power of unified collaboration within—and beyond—the enterprise.

The modular design of the RMX 4000 is based on the Advanced Telecom Computing Architecture (AdvancedTCA®), allowing a standards-based, build-as-you-grow approach to capacity and hot swappable parts for fast field service. It also includes built-in redundant AC/DC power supplies.

The Polycom RMX™ 4000 straight forward user and administrator interface is the same as for the RMX 2000, which increases productivity and speeds the rate of conferencing adoption.

The RMX™ 4000 Real-time Media Conference Platform offers up to 320 video resources and 1600 audio resources. *Flexible Resource Capacity* supports:

- 80 HD endpoints in continuous presence (CP)
- 120 Standard Definition (SD) endpoints in CP (with max resolution of 1024x576)
- 320 CIF endpoints in CP or HD endpoints in Video Switching conference
- 1,600 VoIP endpoints or 400 PSTN.

For detailed description of the RMX 4000 hardware components, see the *Polycom RMX 4000 Hardware Guide*.

Hardware Additions

The RMX 4000 contains new cards and modified components:

- RTM LAN
- RTM IP 4000
- CNTL 4000
- Fabric Switch Module (FSM4000)
- AC/DC Power
- Fan drawer

In addition, up to four MPM+ media cards can be installed in the system.

System Capacities

The increase in the number of MPM+ cards that can be installed in the system increases the overall system capacity. The following table summarizes the different system capacities.

Table 8 *System Functions and Capacities*

System Functions	RMX 2000	RMX 4000
Maximum no. of participants (audio) in a conference	800	800
Maximum number of participants (video) in a conference	160	160
Maximum number of conferences	400	800
Maximum number of Meeting Rooms	1000	2000
Maximum number of Entry Queues	40	80
Maximum number of Profiles	40	80
Maximum number of Conference Templates	100	200
Maximum number of SIP Factories	40	80
Maximum number of IP Services	1	1
Maximum number of ISDN Services	2	2
Maximum number of IVR Services	40	80
Maximum number of Recording Links	1	1
Maximum number of IVR Video Slides	150	150
Maximum number of Reservations (Internal Scheduler)	2000	4000
Maximum number of Log Files (1Mb max.)	4000	8000
Maximum number of CDR Files	2000	4000
Maximum number of Fault Files	1000	1000
Number of Participant alerts	Unlimited	Unlimited
Number of HTTP (Web) clients connected to the MCU	20	20
Maximum number Address Book entries	2000	4000
Maximum number of Users	100	100

Resource Capacities

Table 1-1 summarizes resource capacities per resolution in CP conferencing mode.

Table 1-1 *MPM+ Resource Capacity per Resolution in CP*

Resource Type	Maximum Possible Resources MPM+
HD720p60/HD1080p30 Symmetric	Not Applicable
HD720p60/HD1080p30 Asymmetric	10
HD720p30/ SD 60	20
SD 30 (H.264)/ 4CIF 60	30
4CIF (H.263)	30
CIF (H.264)	80
CIF (H.263)	80
Audio only (VoIP)	400
PSTN Participants	

Table 1-2 summarizes resource capacities per line rate in VSW conferencing mode.

Table 1-2 *MPM+ Resource Capacity per Line Rate in VSW*

Resource Type	Maximum Possible Resources MPM+
VSW 2Mbps	80
VSW 4Mbps	40
VSW 6Mbps	20

Redundancy

The RMX 4000 has a number of built in redundant components:

- Redundant Power Supply:
  - — Redundant AC Power Supply. The RMX 4000 can be fitted with 3 hot swappable power units, two of which supply power and a third provides redundancy. During failure any of the units can be hot swapped, provide two units are on-line. Each power unit is connected by independent cable to the electrical grid.

  Or

  - — Redundant DC power supply. Two units of – 48v connection, one which supplies power and the other is redundant. Each power unit is connected by independent cable to the electrical grid.
- Fans (8 units) and a Field Replaceable Unit (FRU).

All these units report their status to the Shelf Manager.

Network Separation

On the RMX 4000 Media, Signaling and Management networks are physically separated to provide enhanced security. On the RMX 4000 the IP Network Service and the Management Network have been logically and physically separated from each other. In the IP Network Service each IP address is assigned a physical port and media (RTP) inputs are routed directly to a MPM+ card. This provides for a more secure network with greater bandwidth as each media card has its own dedicated port. All signaling communications are processed on a single stack of the Intel Processor on the MCU.

Hardware Monitor Changes

In the RMX 4000, additional slots have been added to the Hardware Monitor section.

Component Slot Allocation

On the RMX™ 4000, components have been assigned dedicated slots as defined in Table 1-3. Slot numbers are located on both the front and rear of the RMX™ 4000.

Table 1-3 *RMX™ 4000 Slot Numbering*

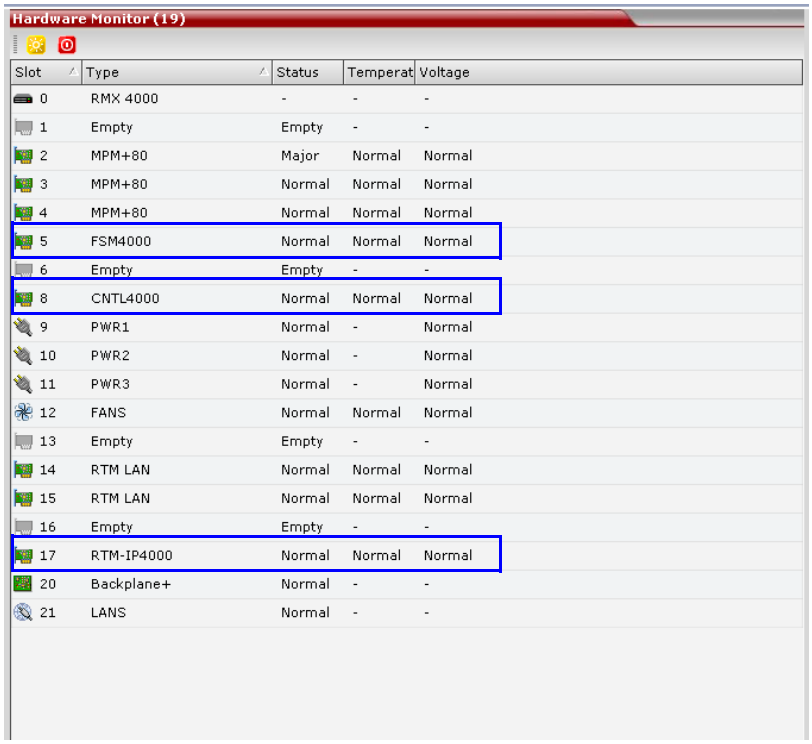
Slot ID/No.	Card/Component	Requirement
1-4	MPM+/MPMx Cards	Mandatory: At least 1 MPM+/MPMxcard is required. Each media card also requires either an RTM ISDN or an RTM LAN card.
5	Fabric Switch Module (FSM 4000)	Mandatory
6	CPU 2	Not Available (NA)
7	Logo Panel	Not Available (NA)
8	CTNL 4000 unit (CPU 1)	Mandatory
9-11	AC Power Supply	An RMX with AC power has 3 power supplies installed. A 3rd power supply is redundant (n+1). Note: Not used with DC powered systems. DC powered systems receive Direct Current from the power rail .
12	Fan Drawer	Mandatory
13-16	RTM ISDN/RTM LAN	Either an RTM ISDN or an RTM LAN card is mandatory in combination with a Media card. The RTM ISDN/RTM LAN board must be inserted in a slot opposite any MPM+/MPMx card.
17	RTM-IP 4000	Mandatory
18	Blank Panel	Not Available (NA)

Table 1-3 RMX™ 4000 Slot Numbering

Slot ID/No.	Card/Component	Requirement
19-21	Power Modules	Mandatory: With AC power, 3 power supplies are installed, with the 3rd redundant. With DC power, 2 power supplies are installed with the 2nd redundant. The center slot (#20) on the rear of the RMX 4000 is disabled and is fitted with blank panel. **Note:** Protective bonding conductor size is 14AWG (1.5mm) within the Power Entry Model.

Hardware Monitor UI Changes

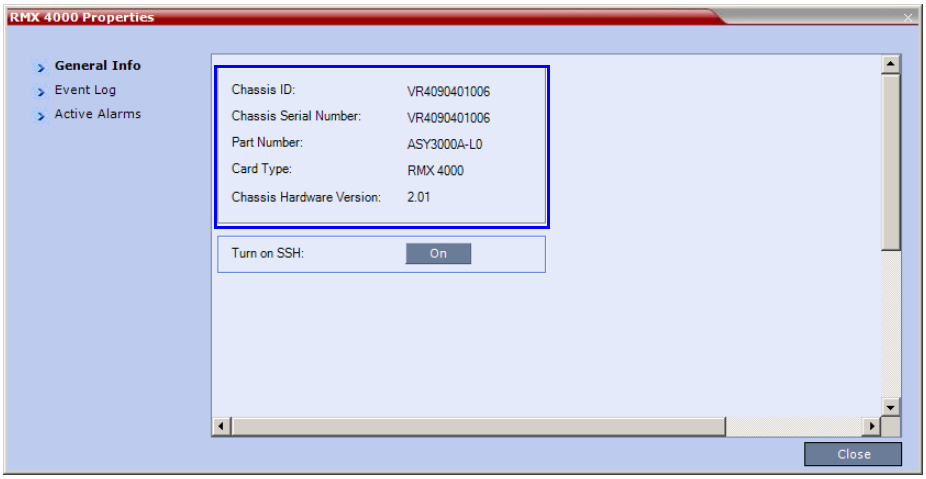
In the *Hardware Monitor* pane, new cards and components are added to the UI:


Hardware Monitor (19)
Slot
Type
Status
Temperat
Voltage
0 RMX 4000 - - -
1 Empty Empty - -
2 MPM+80 Major Normal Normal
3 MPM+80 Normal Normal Normal
4 MPM+80 Normal Normal Normal
5 FSM4000 Normal Normal Normal
6 Empty Empty - -
8 CNTL4000 Normal Normal Normal
9 PWR1 Normal - Normal
10 PWR2 Normal - Normal
11 PWR3 Normal - Normal
12 FANS Normal Normal Normal
13 Empty Empty - -
14 RTM LAN Normal Normal Normal
15 RTM LAN Normal Normal Normal
16 Empty Empty - -
17 RTM-IP4000 Normal Normal Normal
20 Backplane+ Normal - -
21 LANS Normal - -

The Backplan and the LAN slots are numbered incorrectly in the Hardware Monitor list as they should appear without slot numbers as on the RMX 4000 unit. Slots 19 to 21 are incorrectly assigned in the Hardware Monitor and they list should be assigned to the power modules, as on the RMX 4000 unit.

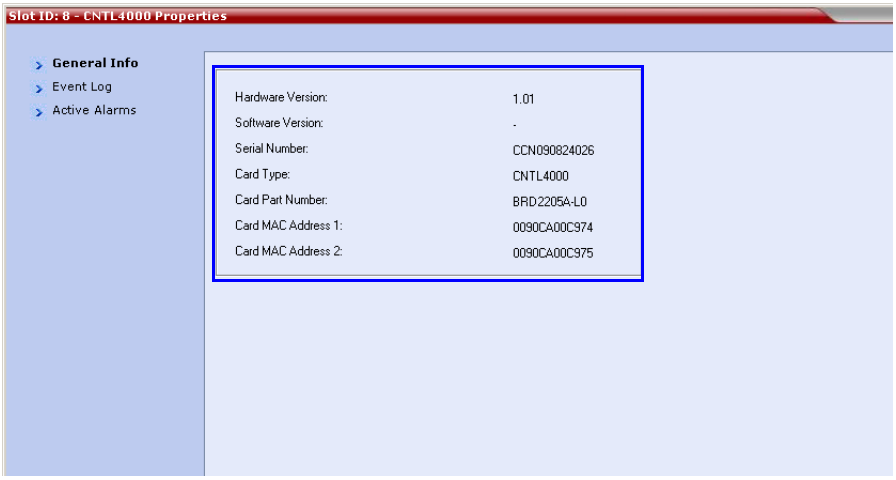
RMX 4000 Properties

The *RMX 4000 Properties - General Info* tab has changed. Fields information is the same as for RMX 2000.



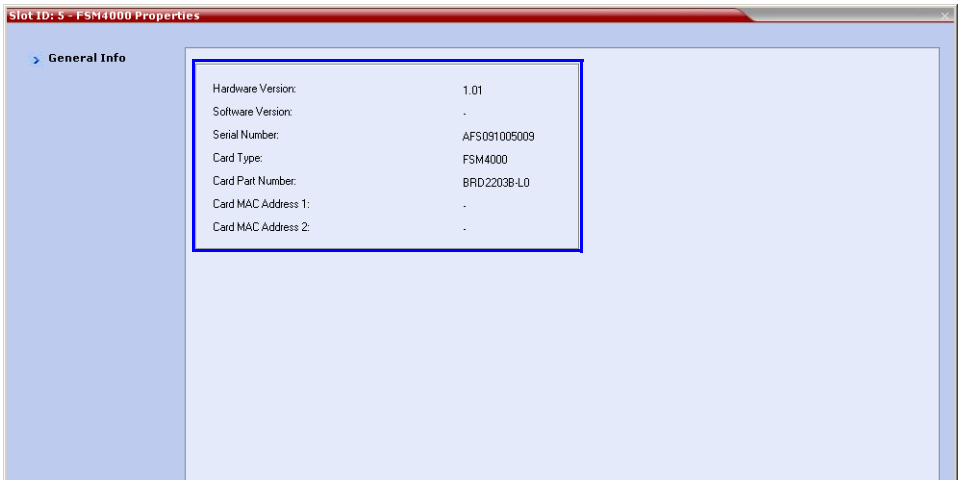
CNTL4000 Properties

The *CTRL4000 Properties - General Info* tab has changed. Fields information is the same as for the RMX 2000 CTRL Module.



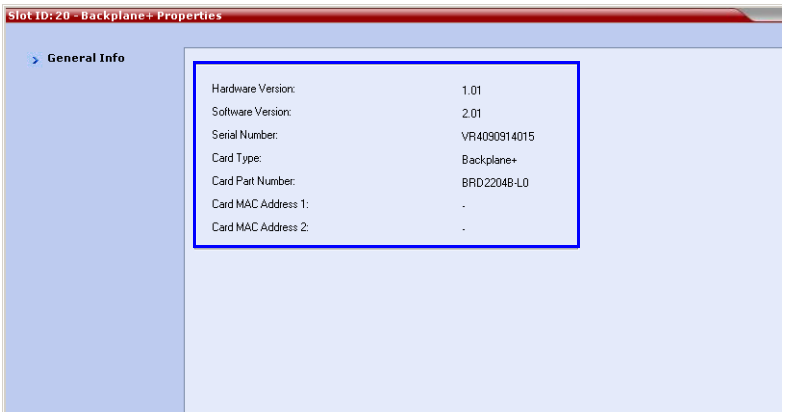
FSM (Fabric Switch Module) 4000 Properties

The Fabric Switch Module (FSM) performs media processing functions on the RMX 4000 unit.



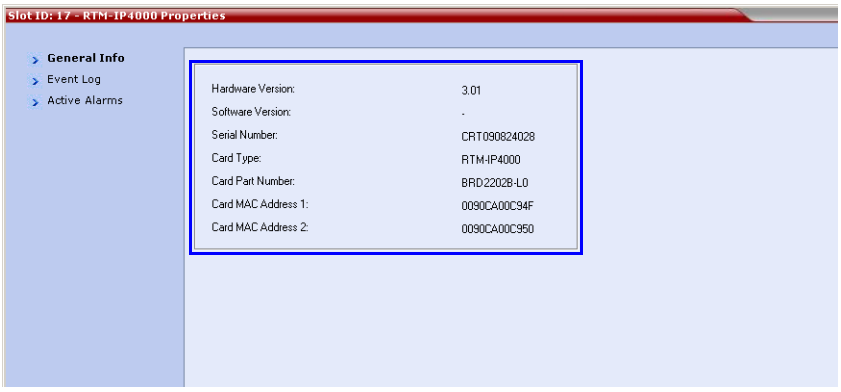
Backplane 4000 Properties

The *Backplane 4000 Properties - General* Info tab has changed. Fields information is the same as for the RMX 2000 Backplane Module.



RTM IP4000 Properties

The *RTM IP4000 Properties - General Info* tab has changed. Fields information is the same as for the RMX 2000 RTM IP Module.

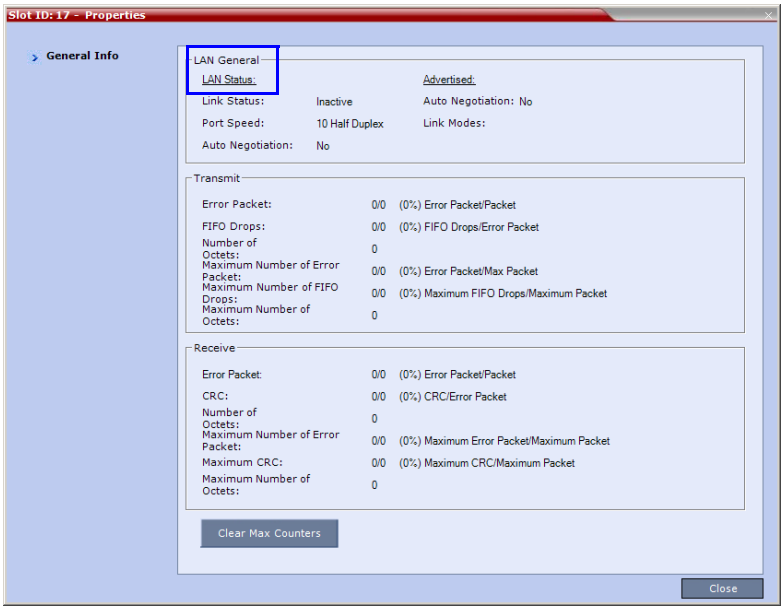


LAN Unit List Properties

The *LAN Unit List* Properties have changed. Additional Ports were added for the new modules.

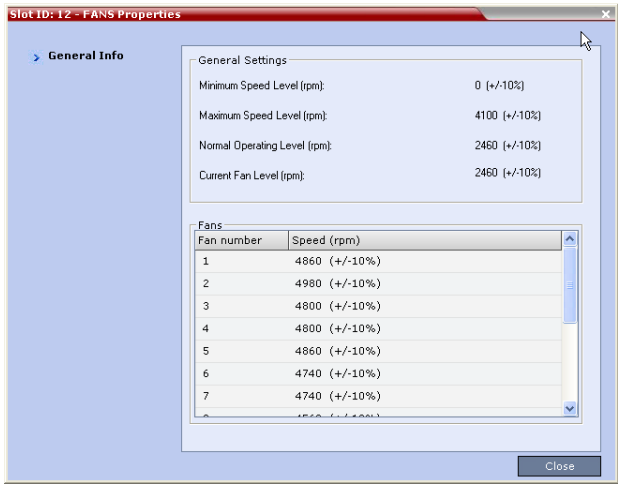
RTM LAN Properties

The *RTM LAN Properties - General Info* tab has changed. Fields information is the same as for the RMX 2000 RTM LAN Module.


Slot ID: 17 - Properties
General Info
LAN General
LAN Status:
Advertised:
Link Status: Inactive
Auto Negotiation: No
Port Speed: 10 Half Duplex
Link Modes:
Auto Negotiation: No
Transmit
Error Packet: 0/0 (0%) Error Packet/Packet
FIFO Drops: 0/0 (0%) FIFO Drops/Error Packet
Number of Octets: 0
Maximum Number of Error Packet: 0/0 (0%) Error Packet/Max Packet
Maximum Number of FIFO Drops: 0/0 (0%) Maximum FIFO Drops/Maximum Packet
Maximum Number of Octets: 0
Receive
Error Packet: 0/0 (0%) Error Packet/Packet
CRC: 0/0 (0%) CRC/Error Packet
Number of Octets: 0
Maximum Number of Error Packet: 0/0 (0%) Maximum Error Packet/Maximum Packet
Maximum CRC: 0/0 (0%) Maximum CRC/Maximum Packet
Maximum Number of Octets: 0
Clear Max Counters
Close

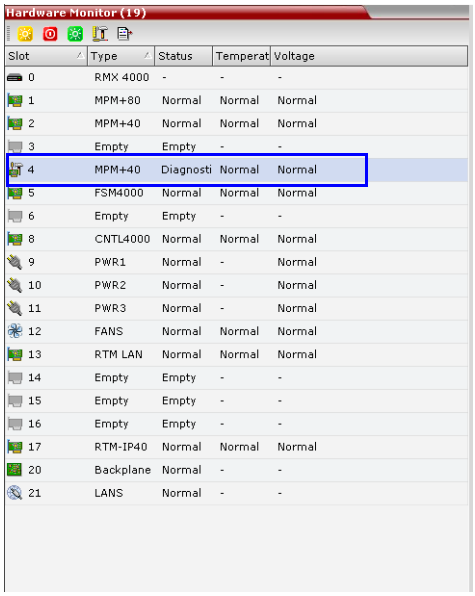
Fans Properties

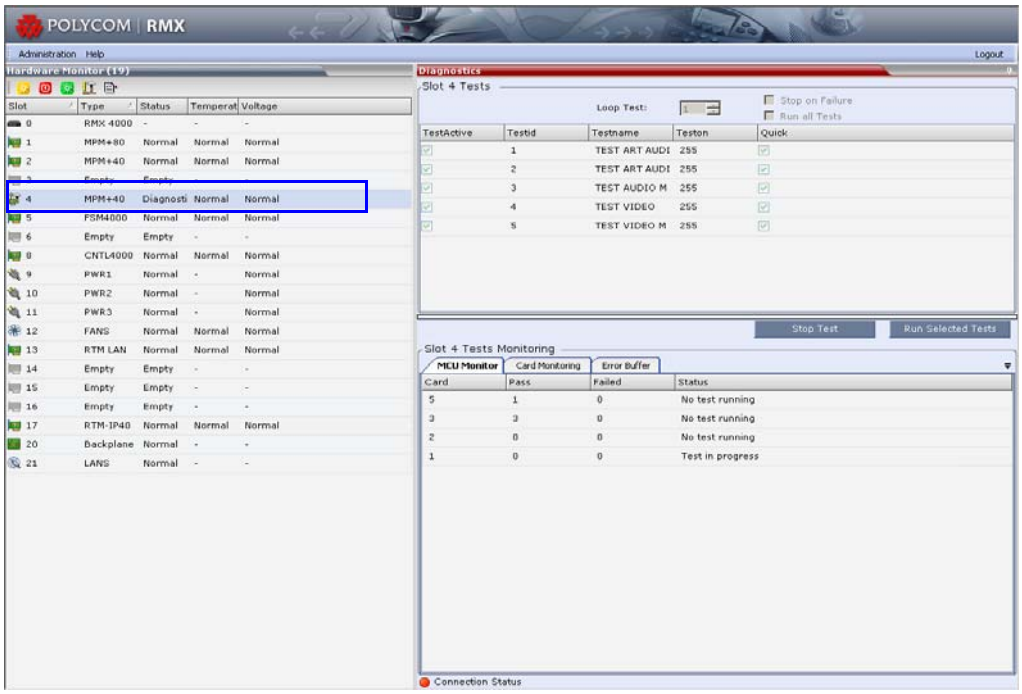
The *Fans - General Info* tab has changed. The Field information is the same as for the RMX 2000 except that the RMX 4000 has a total of 8 Fans.



Hardware Monitor Diagnostic Changes

In the *Hardware Monitor Diagnostics* and *Hardware Monitor Diagnostics Test* panes, the new cards and components are added to the list:


Hardware Monitor (19)
Slot
Type
Status
Temperat
Voltage
0 RMX 4000 - - -
1 MPM+80 Normal Normal Normal
2 MPM+40 Normal Normal Normal
3 Empty Empty - -
4 MPM+40 Diagnosti Normal Normal
5 FSM4000 Normal Normal Normal
6 Empty Empty - -
8 CNTL4000 Normal Normal Normal
9 PWR1 Normal - Normal
10 PWR2 Normal - Normal
11 PWR3 Normal - Normal
12 FANS Normal Normal Normal
13 RTM LAN Normal Normal Normal
14 Empty Empty - -
15 Empty Empty - -
16 Empty Empty - -
17 RTM-IP40 Normal Normal Normal
20 Backplane Normal - -
21 LANS Normal - -



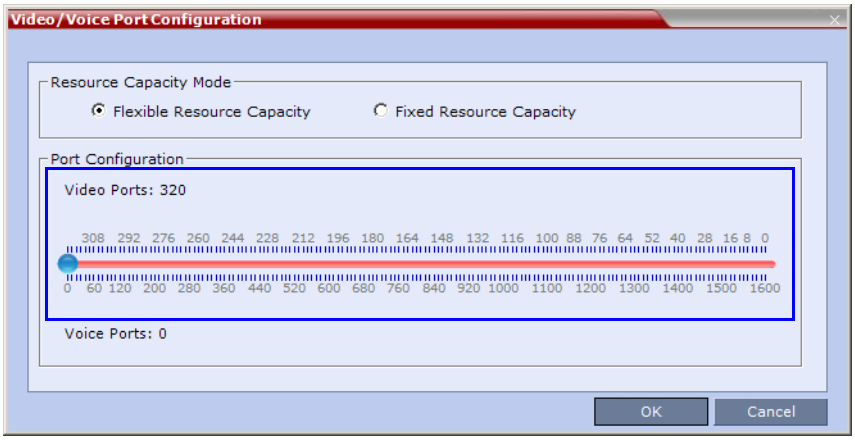
Video/Voice Port Configuration Changes

Changing the *Video/Voice Port Configuration* or switching between *Flexible Resource Capacity* and *Fixed Resource Capacity* modes does not require a system reset. Any change to the Video/Voice Configuration must be performed when there are no active conferences and no connected participants on the RMX.

Flexible Resource Capacity is the default Resource Allocation Mode on the RMX 4000.

The Video and Audio resource capacities on the RMX 4000 have increased for a full system to a maximum of:

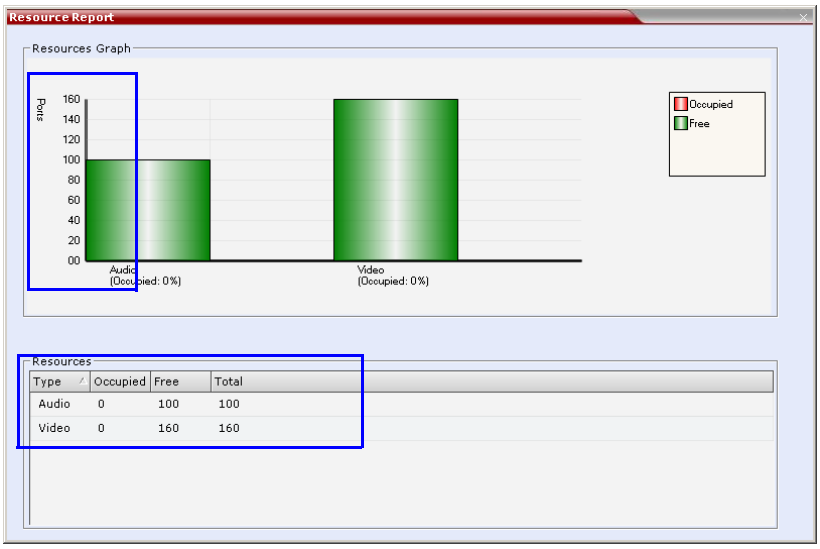
- 320 Video resources
- 1600 Audio resources


Video/Voice Port Configuration
Resource Capacity Mode
Flexible Resource Capacity
Fixed Resource Capacity
Port Configuration
Video Ports: 320
308 292 276 260 244 228 212 196 180 164 148 132 116 100 88 76 64 52 40 28 16 8 0
0 60 120 200 280 360 440 520 600 680 760 840 920 1000 1100 1200 1300 1400 1500 1600
Voice Ports: 0
OK
Cancel

The *Resource Capacity Mode*s are identical to the RMX 2000.

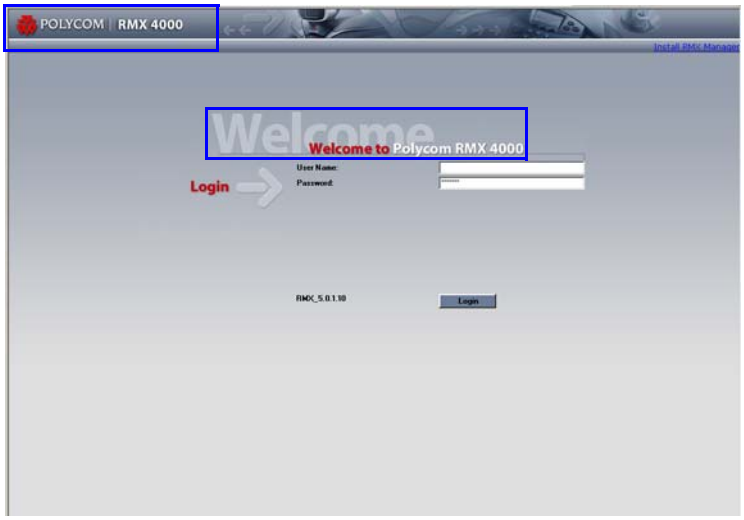
Resource Report Changes

The increased resource capacity of RMX 4000 can be viewed in the Resource Report pane.



RMX 4000 Banner

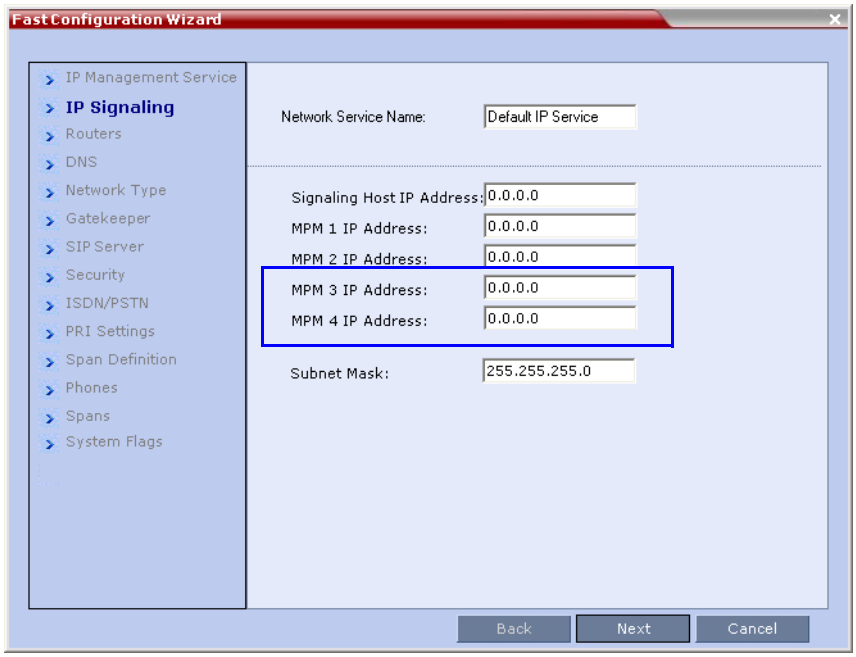
The RMX model (RMX 2000 or RMX 4000) is indicated in the RMX Web Client banner and in the Welcome heading.



Network Service Changes

Fast Configuration Wizard Change

The *Fast Configuration Wizard - IP Signaling* tab has changed. Two new IP Address fields for additional MPM+ slots are added.

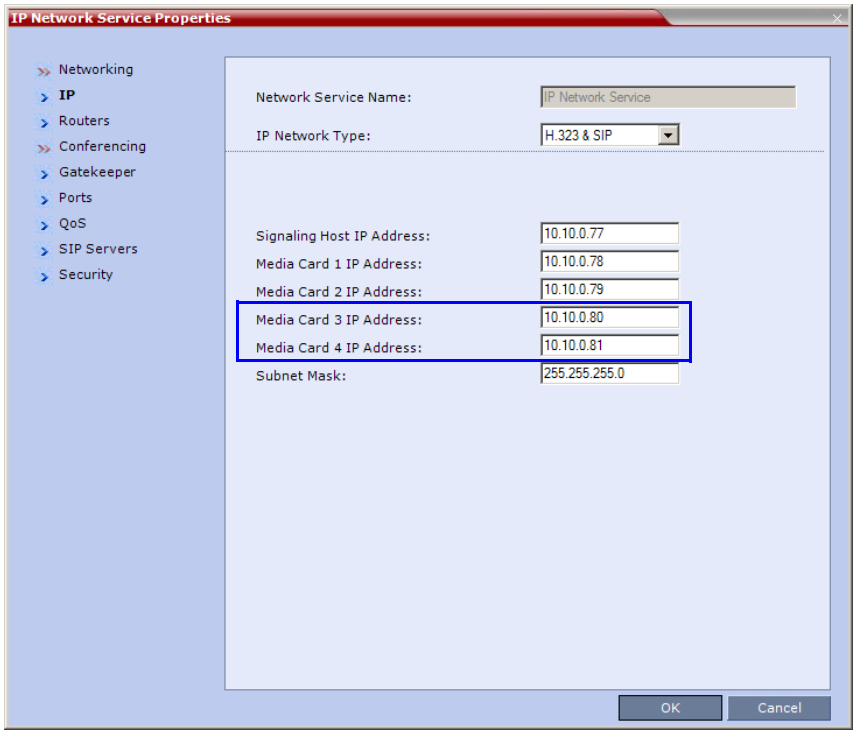


Management Network Change

The configuration of the speed and transmit/receive mode for each LAN port was moved from the Management Network to the *Ethernet Setting* function in the *Setup* menu. For more details, see "*Ethernet Settings*" on page **30**.

IP Service Change

In the RMX 4000 the IP Network Service Properties - IP tab has changed. Two new IP Address fields for additional MPM+ slots are added.

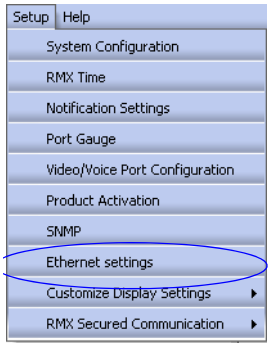


Ethernet Settings

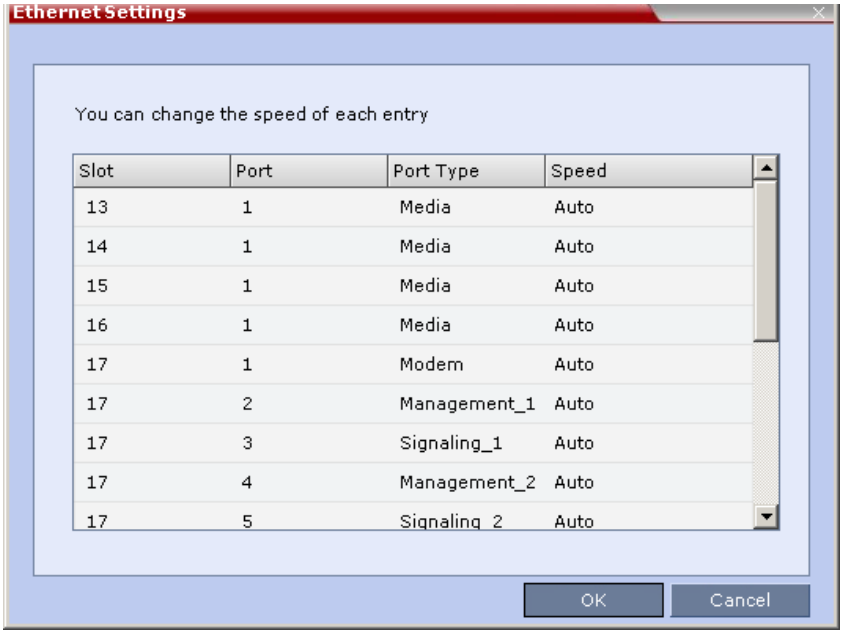
The RMX 4000 is set to automatically identify the speed and transmit/receive mode of each LAN port used by the system. However, these settings may be manually modified if the specific switch requires it.

To modify the automatic LAN port configuration:

1 On the RMX menu, click **Setup > Ethernet Settings**.



The *Ethernet Settings* dialog box opens.



Although the RTM LAN (media card) port is shown as Port 1 in the *Ethernet Settings* and *Hardware Monitor*, the **active LAN connection is Port 2.** LAN 1 is covered with a plastic cap that should not be removed.

2 Modify the following field:

Table 1-4 *Ethernet Settings Parameters*

Field	Description	
Speed	The RMX has 3 LAN ports on the RTM-IP (Management, Signaling and Shelf Management), and additional LAN ports on each media card (RTM LAN) and RTM ISDN cards. The administrator can set the speed and transmit/receive mode manually for these ports.	
	Port	The LAN port number. **Note:** Do not change the automatic setting of Port 1,4 and Port 5 of the Management 2 and Signaling 2 Networks. Any change to the speed of these ports will not be applied.
	Speed	Select the speed and transmit/receive mode for each port. Default: Auto – Negotiation of speed and transmit/receive mode starts at 1000 Mbits/second Full Duplex, proceeding downward to 10 Mbits/second Half Duplex. **Note:** To maximize conferencing performance, especially in high bit rate call environments, a 1Gb connection is recommended.

3 Click **OK**.

Version 5.1.0.G Detailed Description

Audible Alarms

Previously, the RMX users had to rely on visual cues to detect events occurring on the RMX. In *Version 5.1.0.G*, in addition to the visual cues, an audible alarm can be activated and played when participants request Operator Assistance.

Using Audible Alarms

The Audible Alarm functionality for Operator Assistance requests is enabled for each MCU in either the RMX Web Client or RMX Manager.

The Audible Alarm played when Operator Assistance is requested is enabled and selected in the **Setup > Audible Alarm > User Customization**. When the Audible Alarm is activated, the *.wav file selected in the *User Customization* is played, and it is repeated according to the number of repetitions defined in the *User Customization*.

If more than one RMX is monitored in the *RMX Manager*, the Audible Alarm must be enabled separately for each RMX installed in the site/configuration. A different *.wav file can be selected for each MCU.

When multiple Audible Alarms are activated in different conferences or by multiple MCUs, the Audible Alarms are synchronized and played one after the other. It is important to note that when *Stop Repeating Alarm* is selected from the toolbar from the RMX Web Client or RMX Manager, all activated Audible Alarms are immediately halted.

Audible Alarm Permissions

An operator/administrator can configure the Request Operator Assistance audible alarm, however Users with different authorization level have different configuration capabilities as shown in Table 2.

Table 2 *Audible Alarm Permissions*

Option	Operator	Administrator
User Customization	✔	✔
Download Audible Alarm File		✔
Stop Repeating Alarms	✔	✔

Stop Repeating Message

The RMX User can stop playing the audible alarm at any time. If more than one audible alarm has been activated, all activated alarms are immediately stopped.

If after stopping the Audible Alarms a new Operator Assistance request event occurs, the audible alarm is re-activated.

To stop the Audible Alarm on the RMX Client or RMX Manager:

>> On the RMX menu, click **Setup > Audible Alarms >Stop Repeating Alarm**.

When selected all audible alarms are immediately stopped.

Configuring the Audible Alarms

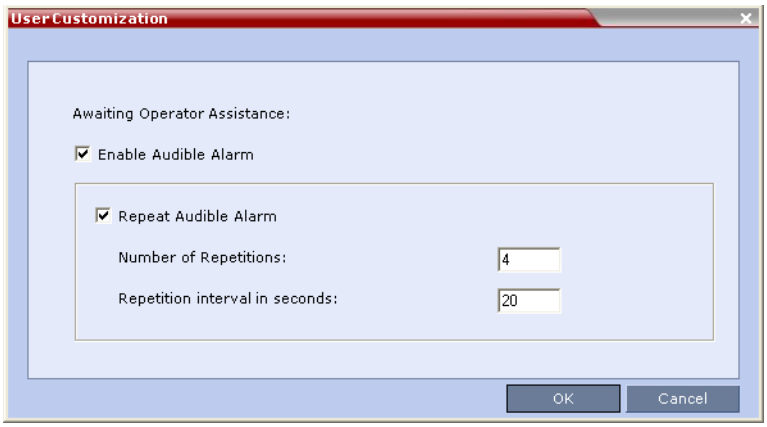
User Customization

The operators and administrators can:

- Enable/Disable the Audible Alarm.
- Select whether to repeat the Audible Alarm.
- Define the number of repetitions and the interval between the repetitions.

To Customize the Audio Alert on the RMX Client or RMX Manager:

1 On the RMX menu, click **Setup** > **Audible Alarms** > **User Customization**.
The *User Customization* window opens.



2 Define the following parameters:

Table 3 *Audible Alarm - User Customization Options*

Option	Description
Enable Audible Alarm	Select this check box to enable the Audible Alarm feature and to define its properties. When this check box is cleared, the Audible Alarm functionality is disabled.
Repeat Audible Alarm	Select this check box to play the Audible Alarm repeatedly. When selected, it enables the definition of the number of repetitions and the interval between repetitions. When cleared, the Audible Alarm will not be repeated and will be played only once.
Number of Repetitions	Define the number of times the audible alarm will be played. Default number of repetitions is 4.
Repetition interval in seconds	Define the number of seconds that the system will wait before playing the Audible Alarm again. Default interval is 20 seconds.

3 Click **OK**.

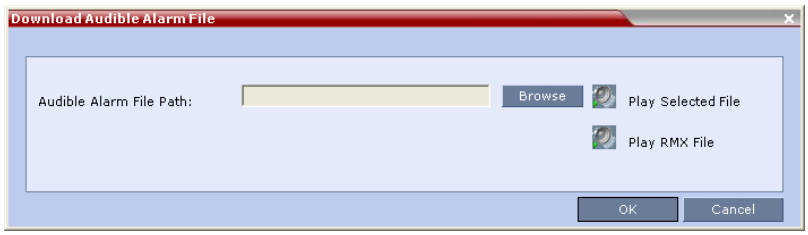
Replacing the Audible Alarm File

Each RMX is shipped with a default tone file in *.wav format that plays a specific tone when participants request Operator Assistance. This file can be replaced by a *.wav file with your own recording. The file must be in *.wav format and its length cannot exceed one hour.

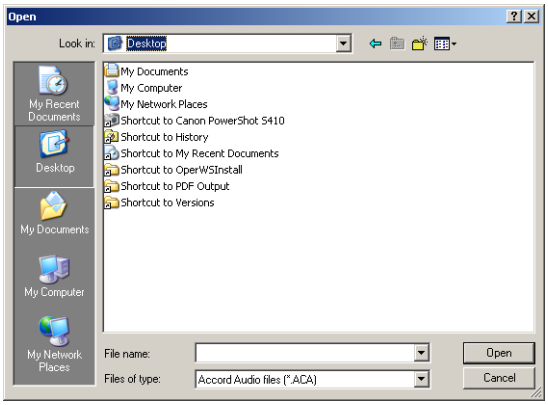
Only the User with Administrator permission can download the Audible Alarm file.

To replace the Audio file on the RMX Client or RMX Manager:

1 On the RMX menu, click **Setup > Audible Alarms > Download Audible Alarm File**.
The *Download Audible Alarm File* window opens.



2 Click the **Browse** button to select the audio file (*.wav) to download.
The *Open* dialog box opens.



3 Select the appropriate *.wav file and then click the **Open** button.
The selected file name appears in the *Install Audible Alarm File* dialog box.

4 **Optional**. You can play the selected file or the currently used file by clicking the *Play* ( ) button as follows:

   a Click **Play Selected File** to play a file saved on your computer.

   b Click **Play RMX File** to play the file currently saved on the RMX.

5 In the *Download Audible Alarm File* dialog box, click **OK** to download the file to the MCU.

The new file replaces the file stored on the MCU. If multiple RMXs are configured in the RMX Manager, the file must be downloaded to each of the required MCUs separately.

Recording Link Encryption

Recording Links can be encrypted when recording an encrypted conference. The encryption of the *Recording Link* is enabled when *Encryption* is selected in the *Conference Profile* on the RMX and on the RSS, and the system flag ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF is set to NO.

When the **JITC_MODE** flag is set to **YES**, this feature is not supported.

Recording Link Encryption Guidelines:

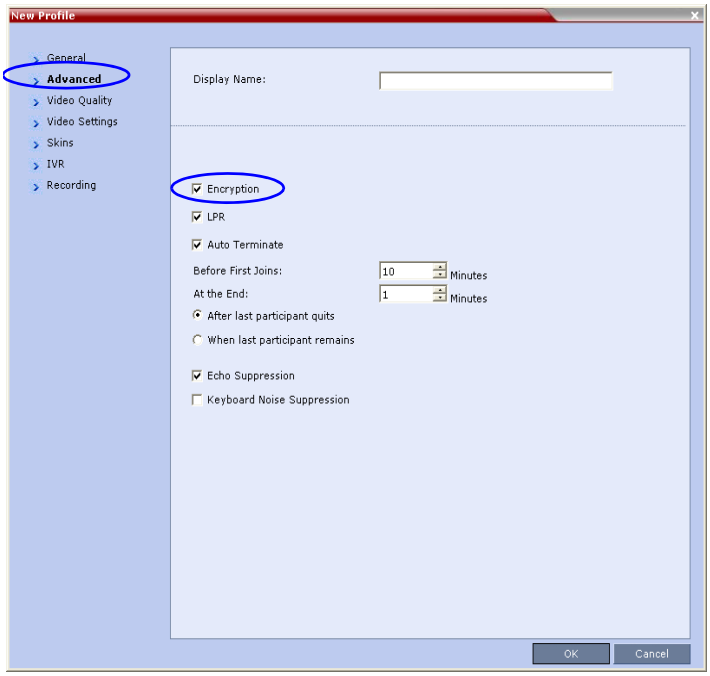
- The Recording Link connection type must be H.323.
- The Recording Link uses the *AES* encryption format.
- The RSS 2000/4000 recorder must be set to support encryption. The following RSS recorders support encryption:
  - RSS 4000 version 5.0 with "upgrade package_1647_Release version" installed
  - RSS 2000 with version 4.0.0.001 360 installed

  For more information refer to the *RSS 2000/4000 User Manual*.
- The system flag ALLOW_NON_ENCRYPT_RECORDING_LINK_ IN_ENCRYPT_CONF is set to NO (default).
- Encryption must be selected in the *Conference Profile*.

Recording Link Settings

The recording of encrypted conferences via an encrypted Recording Link is enabled in the Conference Profile by:

- Selecting the Encryption option in the *Advanced* tab.



- Setting the Recording options in the *Recording* tab

For more information on defining a Recording Link refer to *RMX Administrators Guide*, "*Defining the Recording Link"* on page **11-3**.

However, the flag: ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF can affect the encryption settings of the recording connection/link during a conference.

When the flag is set to NO (default), the Recording Link inherits the encryption settings of the conference. If the conference is encrypted, the recording link will be encrypted.

When the flag is set to YES, it disables the encryption of the recording link, regardless of the Encryption settings of the conference and RSS recorder.

Possible encryption setting of the recording link are summarized in Table 4, "Recording Link Encryption Setting Based on System Configuration Flag Setting".

Table 4 *Recording Link Encryption Setting Based on System Configuration Flag Setting*

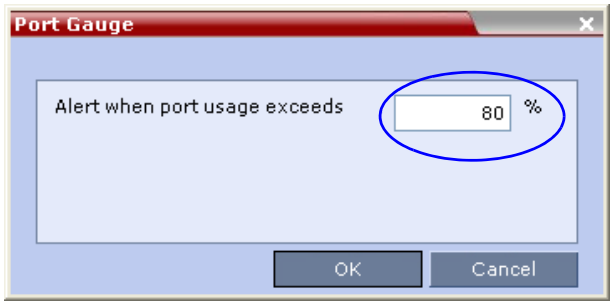
Profile Setting	RSS Setting	Flag Setting	Recording Link Setting
Encryption selected	Encrypted	NO	Encrypted
Encryption selected	Encrypted	YES	Not Encrypted
Encryption selected	Not Encrypted	NO	No connection to the Recorder
Encryption selected	Not Encrypted	YES	Not Encrypted
Encryption not selected	Not Encrypted	YES/NO	Not Encrypted
Encryption not selected	Encrypted	YES/NO	Not Encrypted

SIP Dial-in Busy Notification

When the system flag SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD is set to YES (NO is the default), it enables the RMX to send a busy notification to a SIP audio endpoint or a SIP device when dialing in to the RMX whose audio resource usage exceeded the Port Usage threshold.

The RMX will send a SIP busy response to SIP audio endpoints when:

- The system flag SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD is set to YES (NO is the default)
- The port usage threshold for Audio resources is exceeded. The threshold is defined in the **Setup > Port Gauge** dialog box.



When the flag is set to YES, the system will allow SIP audio endpoints to connect to the MCU until the Port Usage threshold is reached. Once this threshold is exceede, the SIP audio endpoints will not be able to connect, ensuring that the remaining system resources can be used by all other connections, including SIP video, H.323 cascaded links and ISDN video. When the call is rejected by the MCU because of lack of resources, the appropriate indication will be sent by the MCU to the SIP audio endpoint.

For example, if the *Port Gauge* threshold is set to 80%, when 80% of the **Audio resources** are used, the system will not allow additional SIP audio endpoints to connect and will send a busy notification to the endpoint.

This does not affect the video resources usage.

Version 4.5.0.F Detailed Description - General

IPv6 Support

This version includes support for *IPv6*.

Dial in, dial out connections and RMX management are supported within the following IP addressing environments:

- IPv6
- IPv4
- IPv6 & IPv4

When *IPv4* is selected, IPv6 fields are not displayed and conversely when *IPv6* is selected, *IPv4* fields are not displayed. When *IPv6 & IPv4* is selected both *IPv6* and *IPv4* fields are displayed.

For the purposes of comprehensive documentation, all screen captures in this document show the dialog boxes as displayed with *IPv6 & IPv4* selected.

IPv6 Networking Addresses for RMX Internal and External Entities

IPv6 addresses can be assigned to both *RMX* (*Internal*) and *External Entity* addresses.

RMX Internal Addresses

Default Management Network Service

- Control Unit
- Signaling Host
- Shelf Management
- MPM1 (Media Card)
- MPM2 (Media Card)
- MPM3 (Media Card) - RMX 4000
- MPM4 (Media Card) - RMX 4000

External Entities

- Gatekeepers (Primary & Secondary)
- SIP Proxies
- DNS Servers
- Default Router
- Defined participants
- External Database Server

IPv6 Guidelines

- *Internet Explorer 7*™ is required for the *RMX Web Client* and *RMX Manager* to connect to the RMX using *IPv6*.

- *IPv6* is supported with MPM+ media cards only.
- The default IP address version is *IPv4*.
- The IP address field in the *Address Book* entry for a defined participant can be either *IPv4* or *IPv6*. A participant with an IPv4 address cannot be added to an ongoing conference while the RMX is in *IPv6* mode nor can a participant with an *IPv6* address be added while the RMX is in *IPv4* mode.
  An error message, *Bad IP address version*, is displayed and the *New Participant* dialog box remains open so that the participant's address can be entered in the correct format.
- Participants that do not use the same IP address version as the RMX in ongoing conferences launched from *Meeting Rooms*, *Reservations* and *Conference Templates*, and are disconnected. An error message, *Bad IP address version*, is displayed.
- IP Security (IPSec) Protocols are not supported.

Using IPv6 Addressing

Management Network Service

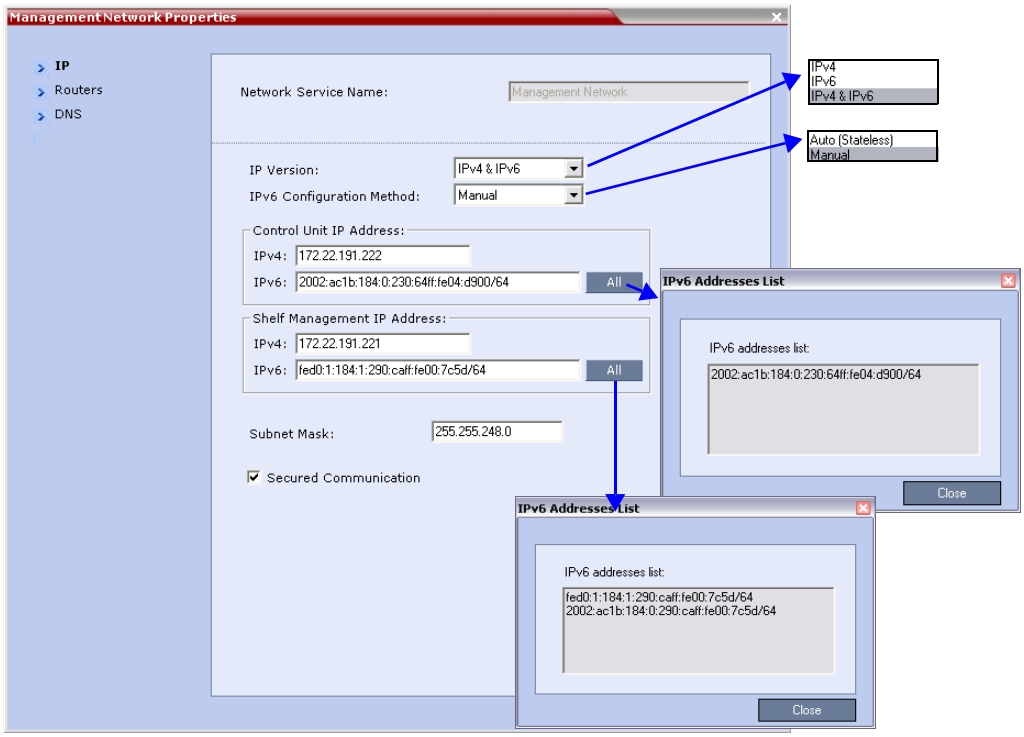
The *Factory Default* IP addressing mode for new MCUs during *First-time Power-up* is *IPv4*. The default IP addressing mode for MCUs that have been upgraded is also *IPv4*.

The MCU is initially configured using the procedure described in the *RMX 2000/4000 Deployment Guide for Maximum Security Environments*, "*Procedure 3: First Entry Configuration*" on page **1-13**. *IPv6* addressing is then enabled by modifying the *Management Network Service*.

To modify the Management Network Service:

1 In the *RMX Management* pane, click the **IP Network Services** ( ) button.

2 In the *IP Network Services* list pane, double-click the **Management Network** ( ) entry. The *Management Network Properties - IP* dialog box opens.



3 Modify the following fields:

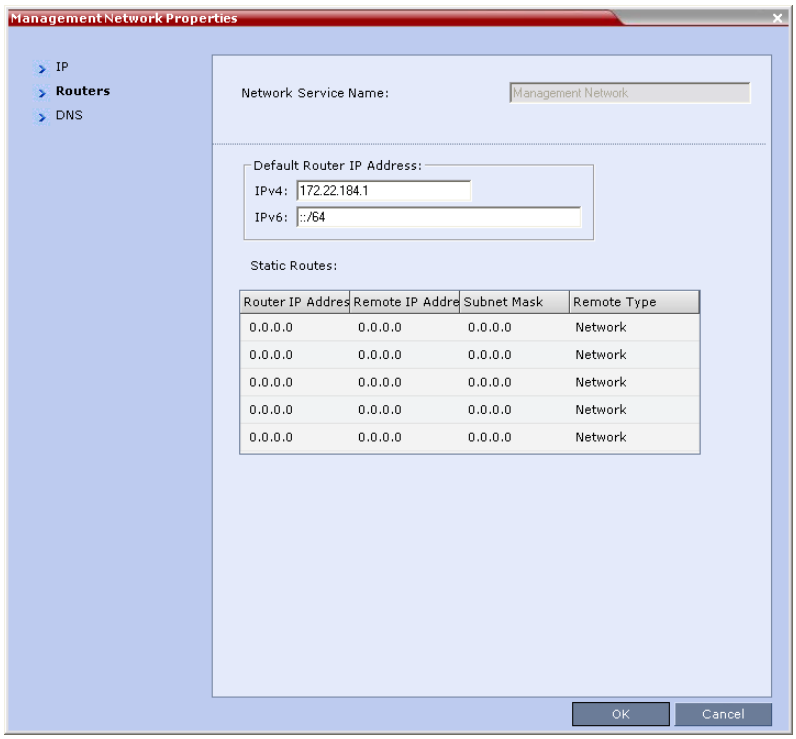
Table 5 *Default Management Network Service – IP*

Field	Description	
Network Service Name	Displays the name of the Management Network. This name cannot be modified. **Note:** This field is displayed in all Management Network Properties tabs.	
IP Version	IPv4	Select this option for IPv4 addressing only.
	IPv6	Select this option for IPv6 addressing only.
	IPv4 & IPv6	Select this option for both IPv4 and IPv6 addressing.
IPv6 Configuration Method	Auto (Stateless)	Select his option to allow automatic generation of the following addresses: • Link-Local (For internal use only) • Site-Local • Global
	Manual	Select his option to enable manual entry of the following addresses: • Site-Local • Global Manual configuration of the following address types is not permitted: • Link-Local • Multicast • Anycast
Control Unit IP Address	IPv4	The IPv4 address of the RMX Control Unit. This IP address is used by the *RMX Web Client* to connect to the RMX.
	IPv6	The IPv6 address of the RMX Control Unit. This IP address is used by the *RMX Web Client* to connect to the RMX. **Note:** *Internet Explorer 7*™ is required for the *RMX Web Client* to connect to the RMX using IPv6.
	All	Click the **All** button to display the *IPv6* addresses as follows: • *Auto* - If selected, *Site-Local* and *Global* site addresses are displayed. • *Manual* if selected, only the *Manual* site address is displayed.

Table 5 *Default Management Network Service – IP*

Field	Description		
Shelf Management IP Address	IPv4	The IPv4 address of the *RMX Shelf Management Server*. This IP address is used by the *RMX Web Client* for *Hardware Monitoring* purposes.	
	IPv6	The IPv6 address of the *RMX Shelf Management Server*. This IP address is used by the *RMX Web Client* for *Hardware Monitoring* purposes. **Note:** *Internet Explorer 7*™ is required for the *RMX Web Client* to connect to the RMX using IPv6.	
		All	Click the **All** button to display the *IPv6* addresses as follows: • *Auto* - If selected, *Site-Local* and *Global* site addresses are displayed. • *Manual* if selected, only the *Manual* site address is displayed.
Subnet Mask	Enter the subnet mask of the Control Unit. **Note:** This field is specific to *IPv4* and is not displayed in *Ipv6* only mode.		
Secured Communication	Select to enable Secured Communication. The RMX supports TLS 1.0 and SSL 3.0 (Secure Socket Layer). A SSL/TLS Certificate must installed on the RMX for this feature to be enabled. For more information see the *RMX 2000/4000 Administrator's Guide for Maximum Security Environments*, "*Secure Communication Mode"* on page **F-1**.		

4 Click the **Routers** tab.

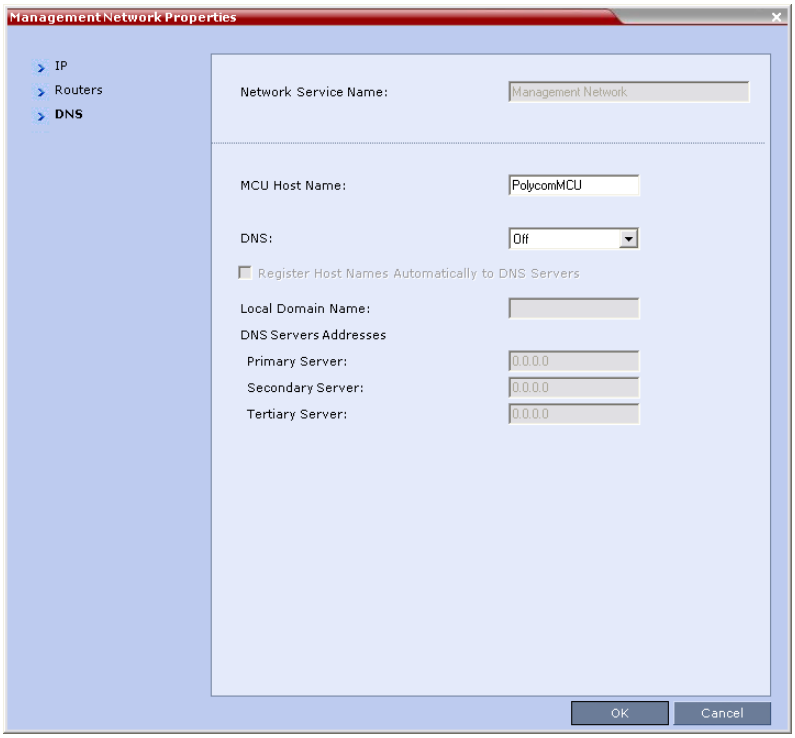


5 Modify the following fields:

Table 6 *Default Management Network Service – Routers*

Field	Description	
Default Router IP Address	IPv4	Enter the IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.
	IPv6	
Static Routes IPv4 Only Table		The system uses *Static Routes* to search other networks for endpoint addresses that are not found on the local LAN. Up to five routers can be defined in addition to the Default Router. The order in which the routers appear in the list determines the order in which the system looks for the endpoints on the various networks. If the address is in the local subnet, no router is used. To define a static route (starting with the first), click the appropriate column and enter the required value.
	Router IP Address	Enter the IP address of the router.
	Remote IP Address	Enter the IP address of the entity to be reached outside the local network. The *Remote Type* determines whether this entity is a specific component (Host) or a network. • If Host is selected in the *Remote Type* field, enter the IP address of the endpoint. • If Network is selected in the *Remote Type* field, enter of the segment of the other network.
	Remote Subnet Mask	Enter the subnet mask of the remote network.
	Remote Type	Select the type of router connection: • **Network** – defines a connection to a router segment in another network. • **Host** – defines a direct connection to an endpoint found on another network.

6 Click the **DNS** tab.

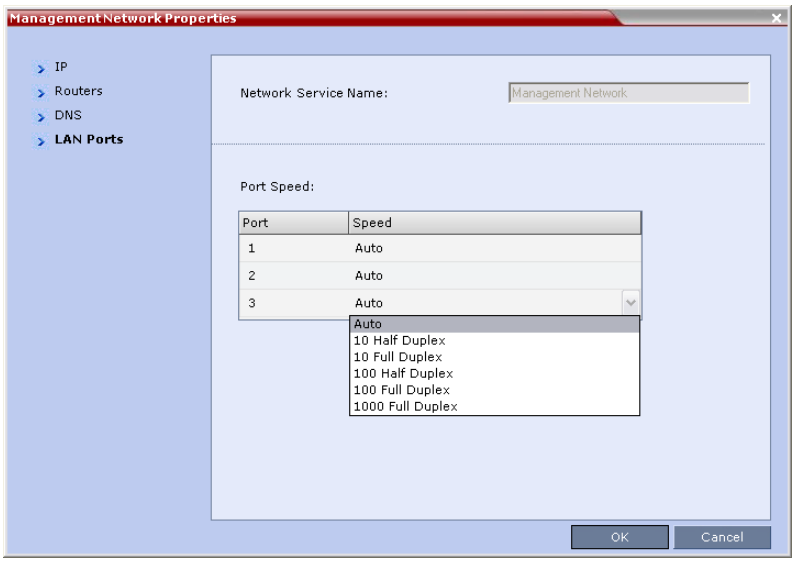


7 Modify the following fields:

Table 1-1 *Default Management Network Service – DNS*

Field	Description
MCU Host Name	Enter the name of the MCU on the network. Default name is RMX
DNS	Select: • **Off** – if DNS servers are not used in the network. • **Specify** – to enter the IP addresses of the DNS servers. **Note:** The IP address fields are enabled only if **Specify** is selected.
Register Host Names Automatically to DNS Servers	Select this option to automatically register the MCU Signaling Host and Shelf Management with the DNS server.
Local Domain Name	Enter the name of the domain where the MCU is installed.
DNS Servers Addresses:	
Primary Server	The static IP addresses of the DNS servers. A maximum of three servers can be defined.
Secondary Server	
Tertiary Server	

8 **RMX 2000 only.** Click the **LAN Ports** tab.



9 Modify the following fields:

Table 1-2 *Default Management Network Service – LAN Ports*

Field	Description	
Port Speed	The RMX has 3 LAN ports. The administrator can set the speed and transmit/receive mode manually for **LAN 2** Port only.	
	Port	The LAN port number: 1, 2 or 3. **Note:** Do not change the automatic setting of Port 1 and Port 3. Only changes to LAN Port 2 speed will be applied.
	Speed	Select the speed and transmit/receive mode for each port. Default: Auto – Negotiation of speed and transmit/receive mode starts at 1000 Mbits/second Full Duplex, proceeding downward to 10 Mbits/second Half Duplex. **Note:** To maximize conferencing performance, especially in high bit rate call environments, a 1Gb connection is recommended.

For setting the LAN ports on the RMX 4000, see "*Ethernet Settings*" on page **30**.

Default IP Network Service

Fast Configuration Wizard

The *Fast Configuration Wizard* enables you to configure the *Default IP Service*. It starts automatically if no *Default IP Network Service* is defined. This happens during *First Time Power-up*, before the service has been defined or if the *Default IP Service* has been deleted, followed by an RMX restart.

The *IP Management Service* tab in the *Fast Configuration Wizard* is enabled only if the factory default *Management IP addresses* were not modified.

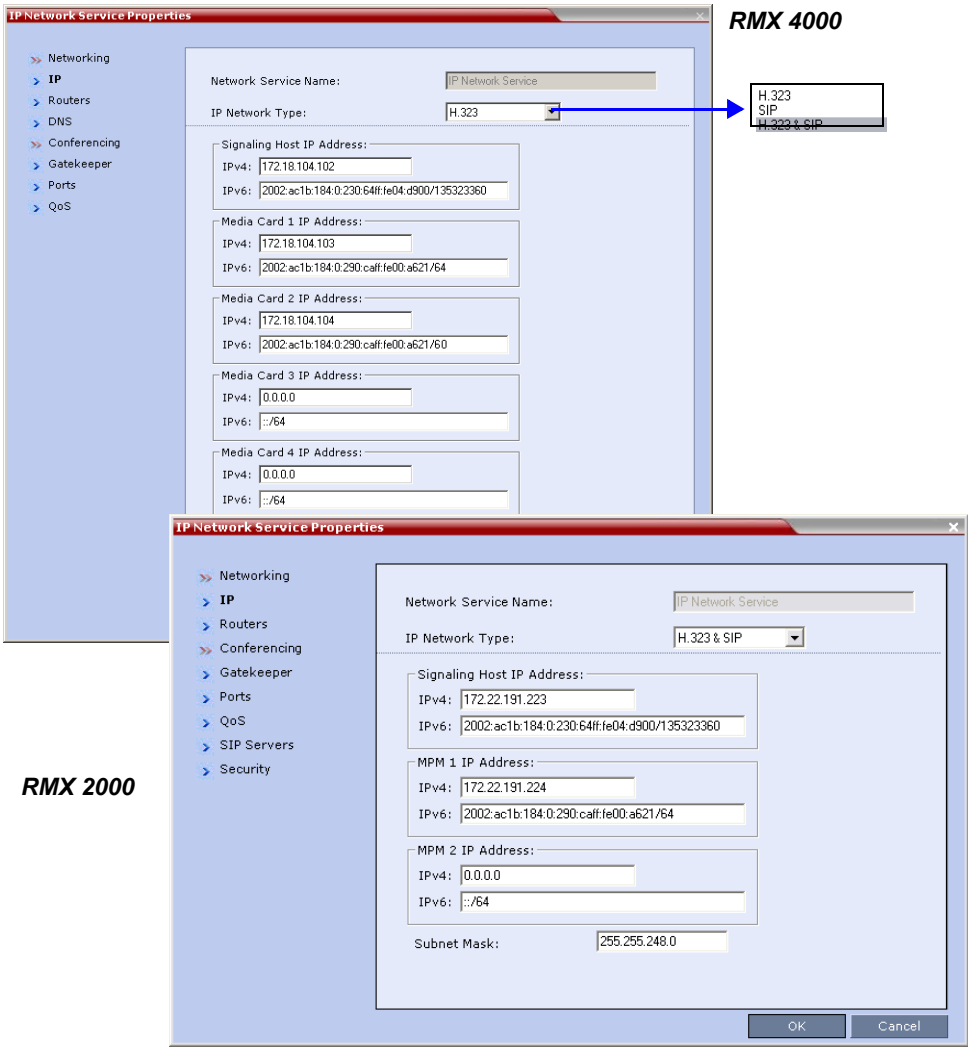
If the *Fast Configuration Wizard* does not start automatically, the *Default IP Service* must be modified through the *IP Network Properties* dialog boxes.

To modify the Default IP Service:

1 In the *RMX Management* pane, click **IP Network Services** ( ).

2 In the *Network* list pane, double-click the **Default IP Service** (, , or) entry.

The *Default IP Service - Networking IP* dialog box opens.



3 Modify the following fields:

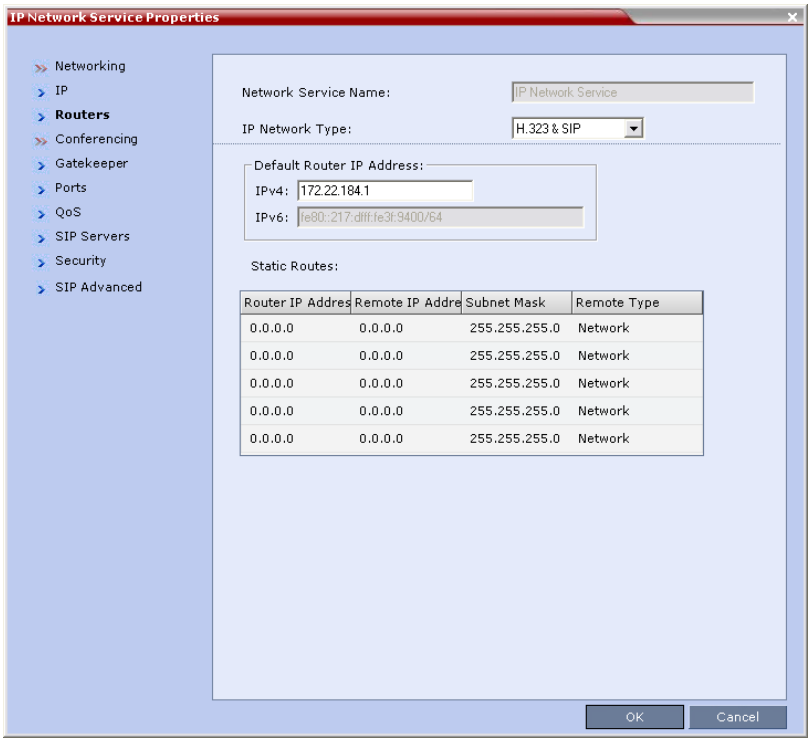
Table 1-3 *Default IP Network Service – IP*

Field	Description
Network Service Name	The name *Default IP Service* is assigned to the IP Network Service by the Fast Configuration Wizard. This name can be changed. **Note:** This field is displayed in all IP Signaling dialog boxes and can contain character sets that use Unicode encoding.

Table 1-3 Default IP Network Service – IP

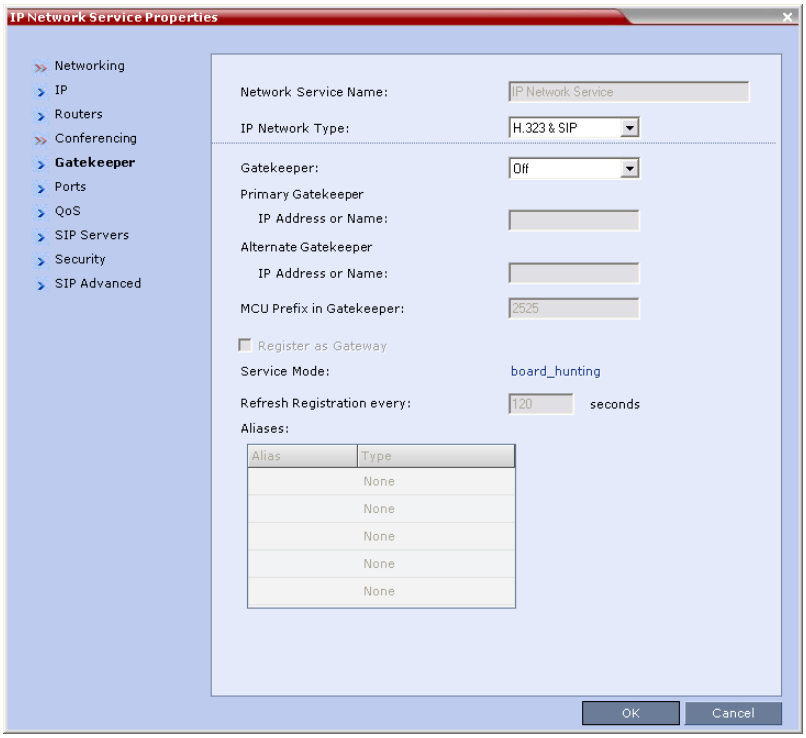
Field	Description
IP Network Type	Displays the network type selected during the First Entry configuration. The Default IP Network icon indicates the selected environment. You can select: • **H.323:** For an H.323-only Network Service. • **SIP:** For a SIP-only Network Service. • **H.323 & SIP:** For an integrated IP Service. Both H.323 and SIP participants can connect to the MCU using this service. **Note:** This field is displayed in all Default IP Service tabs.
Signaling Host IP Address	Enter the address to be used by IP endpoints when dialing in to the MCU. Dial out calls from the RMX are initiated from this address. This address is used to register the RMX with a Gatekeeper or a SIP Proxy server.
Media Card 1 IP Address *Media Card 2 IP Address* *Media Card 3/4 IP Address* **RMX 4000**	Enter the IP address(es) of the media card (s) 1, 2, 3 (RMX 4000) and 4 (RMX 4000), if installed, as provided by the network administrator. Endpoints connect to conferences and transmit call media (video, voice and content) via these addresses.
Subnet Mask **(IPv4 only field)**	Enter the subnet mask of the MCU. Default value: 255.255.255.0.

4 Click the **Routers** tab.



With the exception of *IP Network Type*, the field definitions of the *Routers* tab are the same as for the *Default Management Network*. For more information see page **41**.

5 Click the **Gatekeeper** tab.



6 Modify the following fields:

Table 1-4 *Default IP Service – Conferencing – Gatekeeper Parameters*

Field	Description	
Gatekeeper	Select **Specify** to enable configuration of the gatekeeper IP address. When **Off** is selected, all gatekeeper options are disabled.	
Primary Gatekeeper IP Address or Name	Enter either the gatekeeper's host name as registered in the DNS or IP address.	**Note:** When in *IPv4&IPv6* or in *IPv6* mode, it is easier to use *Names* instead of *IP Addresses*.
Alternate Gatekeeper IP Address or Name	Enter the DNS host name or IP address of the gatekeeper used as a fallback gatekeeper used when the primary gatekeeper is not functioning properly.	
MCU Prefix in Gatekeeper	Enter the number with which this Network Service registers in the gatekeeper. This number is used by H.323 endpoints as the first part of their dial-in string when dialing the MCU. When PathNavigator or SE200 is used, this prefix automatically registers with the gatekeeper. When another gatekeeper is used, this prefix must also be defined in the gatekeeper.	

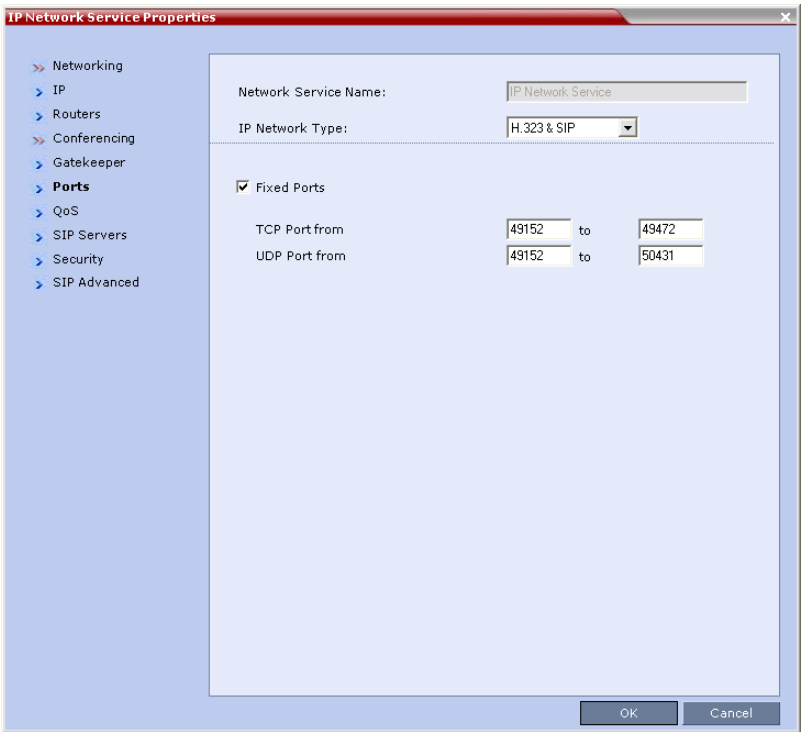
Table 1-4 *Default IP Service – Conferencing – Gatekeeper Parameters*

Field	Description
Register as Gateway	Select this check box if the RMX unit is to be seen as a gateway, for example, when using a Cisco gatekeeper. **Notes:** • When configuring the CMA, this option is initially selected and then is set back to Board Hunting. • Do not use this option when using Radvision gatekeeper.
Refresh Registration every __ seconds	The frequency with which the system informs the gatekeeper that it is active by re-sending the IP address and aliases of the IP cards to the gatekeeper. If the IP card does not register within the defined time interval, the gatekeeper will not refer calls to this IP card until it re-registers. If set to 0, re-registration is disabled. **Note:** • It is recommended to use default settings. • This is a re-registration and not a 'keep alive' operation – an alternate gatekeeper address may be returned.
Aliases:	
Alias	The alias that identifies the RMX's Signaling Host within the network. Up to five aliases can be defined for each RMX. **Note:** When a gatekeeper is specified, at least one prefix or alias must be entered in the table.
Type	The type defines the format in which the card's alias is sent to the gatekeeper. Each alias can be of a different type: • H.323 ID (alphanumeric ID) • E.164 (digits 0-9, * and #) • Email ID (email address format, e.g. abc@example.com) • Participant Number (digits 0-9, * and #) **Note:** Although all types are supported, the type of alias to be used depends on the gatekeeper's capabilities.

7 Click the **Ports** tab.

Settings in the *Ports* tab allow specific ports in the firewall to be allocated to multimedia conference calls.

The port range recommended by IANA (Internet Assigned Numbers Authority) is 49152 to 65535. The MCU uses this recommendation along with the number of licensed ports to calculate the port range.



8 Modify the following fields:

Table 1-5 *Default IP Service – Conferencing – Ports Parameters*

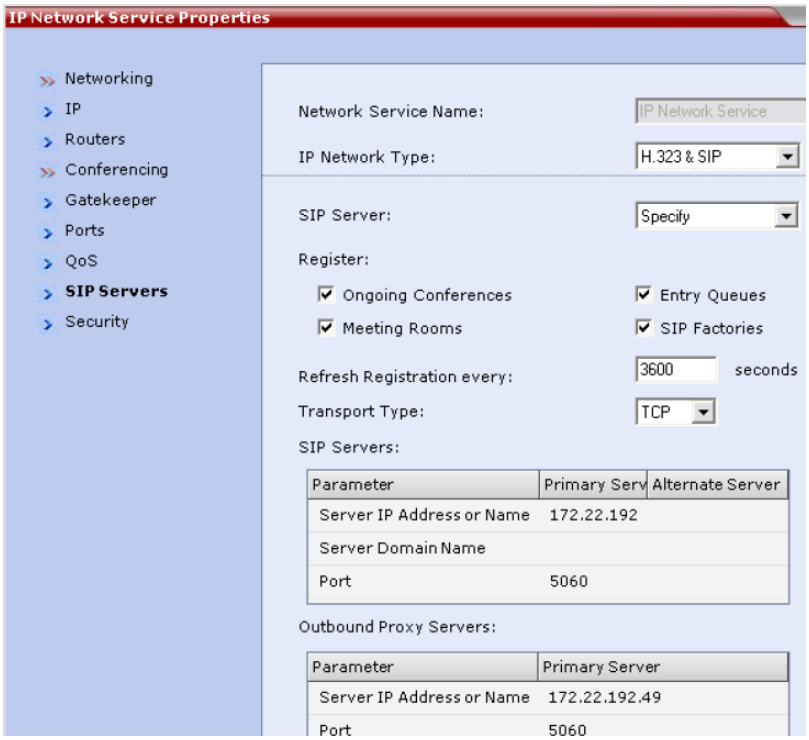
Field	Description
Fixed Ports	Leave this check box clear if you are defining a Network Service for local calls that do not require configuring the firewall to accept calls from external entities. When un-checked, the system uses the default port range. Select this option to enable other port ranges or to limit the number of ports to be left open. When selected, all media ports become fixed ports.
TCP Port from - to	Displays the default settings for port numbers used for signaling and control. To modify the number of TCP ports, enter the first and last port numbers in the range. The number of ports is calculated as follows: Number of simultaneous calls x 2 ports (1 signaling + 1 control).

Table 1-5 Default IP Service – Conferencing – Ports Parameters

Field	Description
UDP Port from - to	Displays the default settings for port numbers used for audio and video. To modify the number of UDP ports, enter the first and last port numbers in the range. The number of ports is calculated as follows: Number of simultaneous calls x 6 ports (2 audio + 4 video).

If the network administrator does not specify an adequate port range, the system will accept the settings and issue a warning. Calls will be rejected when the MCU's ports are exceeded.

9 Click the **SIP Servers** tab.



10 Modify the following fields:

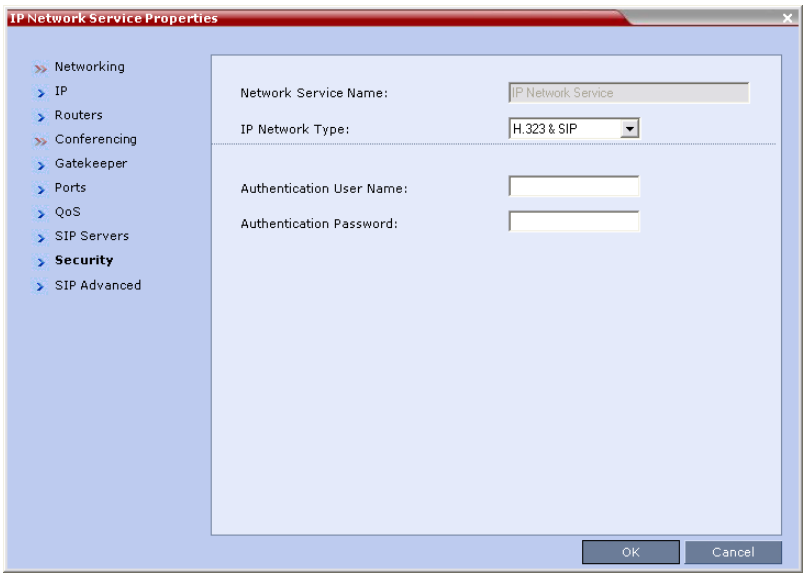
Table 1-6 Default IP Network Service – SIP Servers

Field	Description
SIP Server	Select: • **Specify** – to manually configure SIP servers. • **Off** – if SIP servers are not present in the network.
Register: On going Conferences/ Meeting Rooms/ Entry Queues & SIP Factories	Select the conferencing elements to register with the SIP server. Registering all the conferences and Meeting Rooms with the SIP proxy loads the proxy as the registration is constantly refreshed. It is therefore recommended to register only the Entry Queues and SIP Factories, and use the Entry Queue for conference access.

Table 1-6 *Default IP Network Service – SIP Servers*

Field	Description
Refresh Registration every __ seconds	Enter the frequency in which the system informs the SIP proxy that it is active by re-sending the details of all registered conferencing elements to the server. If the registration is not renewed within the defined time interval, the SIP server will not refer calls to the conferencing entity until it reregisters. If timeout is set to 0, re-registration is disabled. The default value is 3600 seconds (60 minutes).
Transport Type	Select the protocol that is used for signaling between the MCU and the SIP Server or the endpoints according to the protocol supported by the SIP Server: **UDP –** Select this option to use UDP for signaling. **TCP –** Select this option to use TCP for signaling. **TLS –** The *Signaling Host* listens on secured port 5061 only and all outgoing connections are established on secured connections. Calls from SIP clients or servers to non secured ports are rejected. The following protocols are supported: TLS 1.0, SSL 2.0 and SSL 3.0.
SIP Servers: Primary / Alternate Server Parameter	
Server IP Address	Enter the IP address of the preferred SIP server. **Note:** When in IPv4&IPv6 or in IPv6 mode, it is easier to use *Names* instead of *IP Addresses*.
Server Domain Name	Enter the name of the domain that you are using for conferences, for example: `user_name@domain name` The domain name is used for identifying the SIP server in the appropriate domain according to the host part in the dialed string. For example, when a call to `EQ1@polycom.com` reaches its outbound proxy, this proxy looks for the SIP server in the `polycom.com` domain, to which it will forward the call. When this call arrives at the SIP server in `polycom.com`, the server looks for the registered user (EQ1) and forwards the call to this Entry Queue or conference.
Port	Enter the number of the TCP or UDP port used for listening. The port number must match the port number configured in the SIP server. Default port is 5060.
Outbound Proxy Servers: Primary / Alternate Server Parameter	
Server IP Address	By default, the Outbound Proxy Server is the same as the SIP Server. If they differ, modify the IP address of the Outbound Proxy and the listening port number (if required). **Note:** When in IPv4&IPv6 or in IPv6 mode, it is easier to use *Names* instead of *IP Addresses*.
Port	Enter the port number the outbound proxy is listening to. The default port is 5060.

11 Click the **Security** tab.



12 Modify the following fields:

Table 1-7 Default IP Network Service – Security (SIP Digest)

Field	Description
Authentication User Name	Enter the conference, Entry Queue or Meeting Room name as registered with the proxy. This field can contain up to 20 ASCII characters.
Authentication Password	Enter the conference, Entry Queue or Meeting Room password as defined in the proxy. This field can contain up to 20 ASCII characters.

IP Network Monitoring

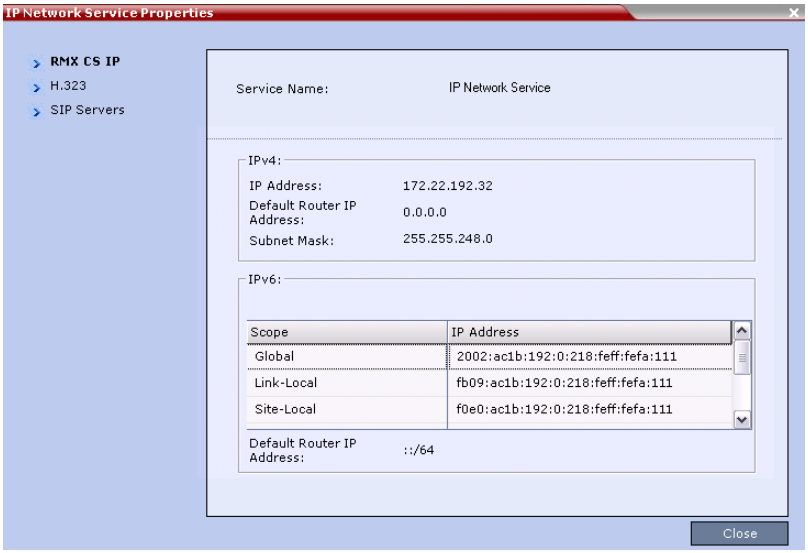
The *Signaling Monitor* is the RMX entity used for monitoring the status of external network entities such as the gatekeeper, DNS, SIP proxy and Outbound proxy and their interaction with the MCU.

To monitor signaling status:

1 In the *RMX Management* pane, click **Signaling Monitor** ( ).

2 In the *Signaling Monitor* pane, double-click **Default IP Service**.

The *IP Network Services Properties – RMX CS IP* tab opens:

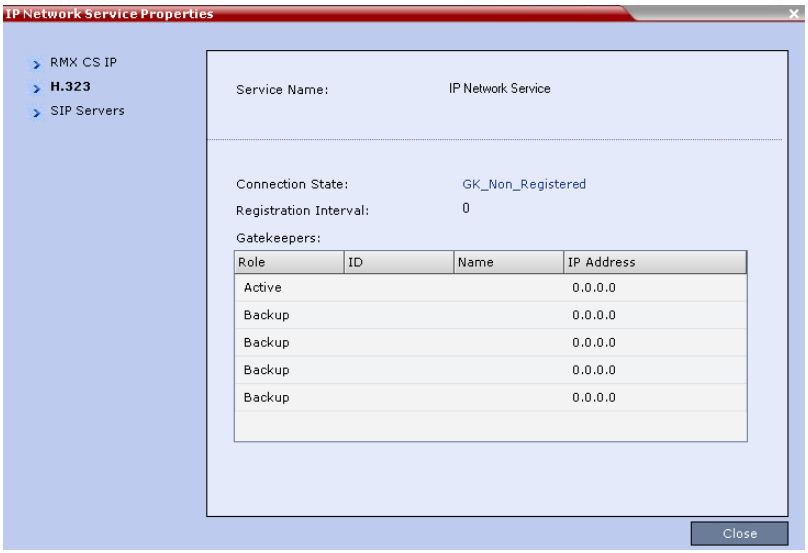


The *RMX CS IP* tab displays the following fields:

Table 1-8 *IP Network Services Properties – RMX CS IP*

Field	Description		
Service Name	The name assigned to the *IP Network Service* by the *Fast Configuration Wizard*.		
IPv4	IP Address		
	Default Router IP Address	The IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.	
	Subnet Mask	The subnet mask of the MCU. Default value: 255.255.255.0.	
IPv6	Scope	*IP Address*	
		Global	The Global Unicast IP address of the RMX.
		Site-Local	The IP address of the RMX within the local site or organization.
	Default Router IP Address	The IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.	

3 Click the **H.323** tab.

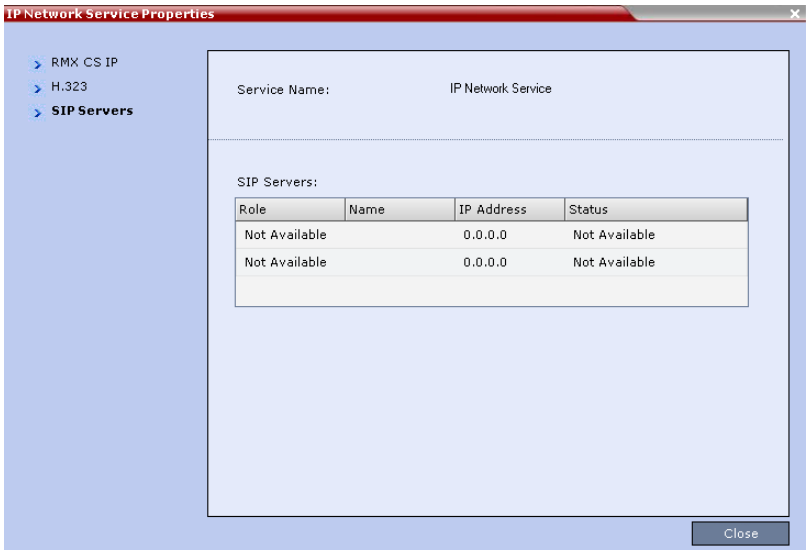


The *H.323* tab displays the following fields:

Table 1-9 *IP Network Services Properties – H.323*

Field	Description	
Connection State	The state of the connection between the Signaling Host and the gatekeeper: **Discovery** - The Signaling Host is attempting to locate the gatekeeper. **Registration** - The Signaling Host is in the process of registering with the gatekeeper. **Registered** - The Signaling Host is registered with the gatekeeper. **Not Registered** - The registration of the Signaling Host with the gatekeeper failed.	
Registration Interval	The interval in seconds between the Signaling Host's registration messages to the gatekeeper. This value is taken from either the IP Network Service or from the gatekeeper during registration. The lesser value of the two is chosen.	
	Role	**Active** - The active gatekeeper. **Backup** - The backup gatekeeper that can be used if the connection to the preferred gatekeeper fails.
	ID	The gatekeeper ID retrieved from the gatekeeper during the registration process.
	Name	The gatekeeper's host's name.
	IP Address	The gatekeeper's IP address.

4 Click the **SIP Servers** tab.



The *SIP Servers* tab displays the following fields:

Table 1-10 *IP Network Services Properties – SIP Servers*

Field	Description
Role	**Active** -The default SIP Server is used for SIP traffic. **Backup** -The SIP Server is used for SIP traffic if the preferred proxy fails.
Name	The name of the SIP Server.
IP	The SIP Server's IP address.
Status	The connection state between the SIP Server and the Signaling Host. **Not Available** - No SIP server is available. **Auto** - Gets information from DHCP, if used.

H.320 Encryption

Media Encryption for *ISDN/PSTN* participants is supported in Version 5.0. Audio, Video and Content channels are encrypted.

Media Encryption for *ISDN/PSTN* participants uses the *AES 128 (Advanced Encryption Standard*) and is fully *H.233/H.234* compliant.

Encryption Key exchange is implemented using the *DH 1024-bit (Diffie-Hellman)* cryptographic protocol.

This *Media Encryption* for *ISDN/PSTN* participants is implemented in RMX systems with MPM+ cards only.

For more information see the *RMX 2000/4000 Administrator's Guide for Maximum Security Environments*, *"Media Encryption"* on page **2-30**.

Media Encryption Guidelines

- Endpoints connecting to an encrypted conference must support both *AES 128* encryption and *DH 1024* key exchange standards and must be *H.233/H.234* compliant.
- *AES Encryption* is set in the profile of conferences, Meeting Rooms, Entry Queues and SIP Factories. The *Encryption* setting cannot be changed while a conference is ongoing.
- *AES Encryption* settings for defined participants can be changed while the participant is disconnected. If the setting is *Auto* (default) the endpoint connects according to the conference *Encryption* setting.
- Participants with an *AES Encryption* setting that does not match that of the conference's *AES Encryption* setting cannot connect to the conference.
- If an endpoint connected to an encrypted conference stops encrypting its media it is disconnected from the conference.
- *Media Encryption* for *H.320* participants is not supported in cascaded conferences.
- The `ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF` *System Flag* determines whether both encrypted and non-encrypted participants (defined and undefined) can connect to a conference and if participants connecting to an Entry Queue can be moved to their destination conference.

  The default value of the flag is **NO**. It can be modified via the **Setup > System Configuration** menu. For more information see the *RMX 2000/4000 Administrator's Guide for Maximum Security Environments*, *"Modifying System Flags"* on page **14-22**.

  When set to **YES**, non-encrypted defined participants are allowed to connect to an encrypted conference.

  Table 2 summarizes the participant ability to connect to the conference according to the flag setting and the conference encryption setting.

Table 2 *Participant Connection to the Conference Based on the Encryption Settings*

ALLOW_NON_ ENCRYPT_PARTY_ IN_ENCRYPT_CONF	Conference Encryption Setting	Participant Encryption Setting	Participant Connection Permitted
NO	Yes	Auto	Yes
NO	Yes	No	No
NO	Yes	Yes	Yes

Table 2 *Participant Connection to the Conference Based on the Encryption Settings*

ALLOW_NON_ ENCRYPT_PARTY_ IN_ENCRYPT_CONF	Conference Encryption Setting	Participant Encryption Setting	Participant Connection Permitted
NO	No	Auto	Yes
NO	No	No	Yes
NO	No	Yes	Yes
YES	Yes	Auto	Yes
YES	Yes	No	Yes
YES	Yes	Yes	Yes
YES	No	Auto	Yes
YES	No	No	Yes
YES	No	Yes	Yes

When an undefined participant connects to an Entry Queue the participant inherits the encryption characteristics of the Entry Queue as defined in the Entry Queue's profile. The participant's move to the destination conference will be successful depending on the Encryption flag setting and the destination conference encryption setting, as summarized in Table 3.

Table 3 *Encryption: Flag vs. Conference and Entry Queue Settings When Participant Encryption is set to Auto*

ALLOW_NON_ ENCRYPT_PARTY_ IN_ENCRYPT_CONF	Entry Queue Encryption Setting	Destination Conference Encryption Setting	Enable Participant Move from EQ to Conference
NO	Yes	No	Yes
NO	Yes	Yes	Yes
NO	No	No	Yes
NO	No	Yes	No
YES	Yes	No	Yes
YES	Yes	Yes	Yes
YES	No	No	Yes
YES	No	Yes	Yes

Ping RMX

The *Ping* administration tool enables the *RMX Signaling Host* to test network connectivity by *Pinging* IP addresses.

Guidelines

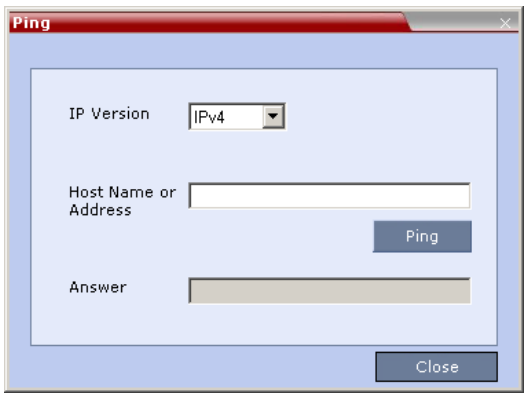
- The IP addressing mode can be either *Ipv4* or *Ipv6*.
- Both explicit IP addresses and *Host Names* are supported.
- The *RMX Web Client* blocks any attempt to issue another *Ping* command before the current *Ping* command has completed. Multiple *Ping* commands issued simultaneously from multiple *RMX Web Client*s are also blocked.

Using Ping

To Ping a network entity from the RMX:

1 On the *RMX* menu, click **Administration > Tools > Ping**.

The *Ping* dialog box is displayed:



2 Modify or complete the following fields:

***Table 4** Ping*

Field	Description
IP Version	Select *IPv4* or *IPv6* from the drop-down menu.
Host Name or Address	Enter the *Host Name* or *IP Address* of the *network* entity to be *Pinged*.

3 Click the **Ping** button.

The *Ping* request is sent to the *Host Name* or *IP Address* of the *RMX* entity.

The *Answer* is either:

— *OK*

or

— *FAILED*

Version 4.5.0.F Detailed Description - Security Enhancements

Enhanced Security Mode (JITC_MODE)

The RMX can operate in one of two modes: standard mode (*Non-JITC Mode)* or *Enhanced Security Mode* (*JITC Mode)*. In the *Enhanced Security Mode* the enhanced security features of the version are rigorously enforced. The *Enhanced Security Mode* is enabled or disabled depending on the value of the **JITC_MODE** *System Flag*.

JITC_MODE System Flag

The **JITC_MODE** *System Flag* affects the ranges and defaults of the S*ystem Flags* that control:

- Network Security
- User Management
- Strong Passwords
- Login and Session Management
- Cyclic File Systems

The Enhanced Security Mode (*JITC mode)* is disabled by default and can be enabled by changing the value of the **JITC_MODE** *System Flag* to **YES** during *First Entry Configuration* or at any time using the **Setup > System Configuration** menu. After modifying the value of the **JITC_MODE** *System Flag* to **YES**, all *RMX* users are forced to change their *Login* passwords.

For more information see the *RMX 2000/4000 Administrator's Guide*, *RMX 2000/4000 Administrator's Guide for Maximum Security Environments*, "*Modifying System Flags*" on page **14-22**.. Table 5 summarizes the interaction between the **JITC_MODE** *System Flag* and the following S*ystem Flags*:

Table 5 *JITC_MODE Flag Value – Effect on System Flags*

Flag	JITC_MODE =			
	YES		NO	
	Range	Default	Range	Default
Network Security				
SEPARATE_MANAGEMENT_NETWORK	YES/ NO	YES	NO	NO
User Management				
DISABLE_INACTIVE_USER	1-90	30	0-90	0

Table 5 *JITC_MODE Flag Value – Effect on System Flags*

Flag	JITC_MODE =			
	YES		NO	
	Range	Default	Range	Default
Session Management				
APACHE_KEEP_ALIVE_TIMEOUT	1-999	15	1-999	120
SESSION_TIMEOUT_IN_MINUTES	1-999	15	0-999	0
USER_LOCKOUT	YES/ NO	YES	YES/ NO	NO
USER_LOCKOUT_WINDOW_IN_MINUTES	0-45000	60	0-45000	60
LAST_LOGIN_ATTEMPTS	YES/ NO	YES	YES/ NO	NO
USER_LOCKOUT_DURATION_IN_MINUTES	0-480	0	0-480	0
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER	4-80	10	4-80	10
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM	4-80	80	4-80	80
Password Management				
FORCE_STRONG_PASSWORD_POLICY	YES	YES	YES/NO	NO
MIN_PASSWORD_LENGTH	15-20	15	0-20	0
NUMERIC_CONF_PASS_MIN_LEN	9-16	9	0-16	0
NUMERIC_CHAIR_PASS_MIN_LEN	9-16	9	0-16	0

Table 5 JITC_MODE Flag Value – Effect on System Flags

Flag	JITC_MODE =			
	YES		NO	
	Range	Default	Range	Default
HIDE_CONFERENCE_PASSWORD	YES/NO	NO	YES/NO	NO
PASSWORD_HISTORY_SIZE	10-16	10	0-16	0
PASSWORD_EXPIRATION_DAYS	7-90	60	0-90	0
PASSWORD_EXPIRATION_WARNING_DAYS	7-14	7	0-14	0
MIN_PWD_CHANGE_FREQUENCY_IN_DAYS	1-7	1	0-7	0
HIDE_CONFERENCE_PASSWORD	YES/NO	NO	YES/NO	NO
Cyclic File Systems				
ENABLE_CYCLIC_FILE_SYSTEM_ALARMS	YES/NO	YES	YES/NO	NO

Force Secured Communications Mode

If the **JITC_MODE** *System Flag* is set to **YES,** a valid **TLS** certificate must be installed, and a secured connection between the *RMX Web Client* (or *RMX Manager*) and the *RMX* unit must be defined.

- If the **JITC_MODE** *System Flag* is set to **YES** and the *Management Network Service* has not yet been configured to be secured, an *Active Alarm* is created and a message is displayed stating that *Secured Communications Mode* must be enabled.
- If the **JITC_MODE** *System Flag* is set to **YES** and a valid TLS certificate has not been installed, an *Active Alarm* is created and a message is displayed stating that the system is in JITC Mode but *Secured Communications Mode* is not enabled until the TLS certificate is installed.
- If the **JITC_MODE** *System Flag* is set to **YES** and *Secured Communications Mode* is enabled, the user is not able to disable *Secured Communications Mode*. An error message is displayed stating that *Secured Communications Mode* cannot be disabled while in *JITC Mode*.
- *TLS* private keys saved by the current version when the **JITC_MODE** *System Flag* is set to **YES** are not compatible with *TLS* private keys saved by previous *RMX*

versions. An *Active Alarm* is created and a message is displayed requesting that a new *TLS* certificate be installed.

- *TLS* private keys saved by the current version will be compatible with *TLS* private keys saved by future *RMX* versions.

Restricted File Uploading

The types of files that can be uploaded to specific folders is restricted.

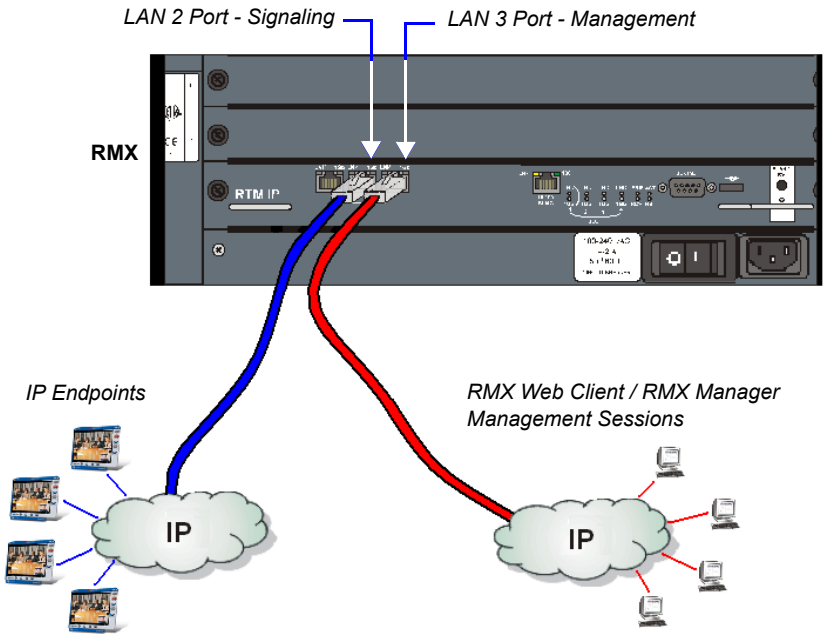
Table 6 *File Upload Restrictions*

Folder	Allowed File Types
/Install/	.bin
/IVR/	.wav .jpg .jpeg .slide
/EMACfg/	.xml
/Restore/	.bck

Network Security

Signaling and Management Network Separation

Network security is enhanced by separating the *Signaling* and *Management Networks*. *Network Separation* is enabled/disabled according to the settings of the **SEPARATE_MANAGEMENT_NETWORK and JITC_MODE** *System Flags*. When both *System Flags* are set to **YES**, all signaling between IP endpoints and the *RMX* is via the **LAN 2** port, while all *RMX* management sessions are hosted via the **LAN 3** port.



This option is implemented in RMX 2000 systems with MPM+ cards only. For details about Network Separation in the RMX 4000, see page 22.

Banner Display and Customization

The *Login Screen* and *Main Screen* of the *RMX Web Client* and the *RMX Manager can* display informative or warning text banners. These banners can include general information or they can be cautioning users to the terms and conditions under which they may log into and access the system, as required in many secured environments.

Banner display is enabled in the *Setup* > *Customize Display Settings* > *Banners Configuration*.

When the **JITC_MODE** *System Flag* is set to **YES**, the banners are displayed by default and cannot be disabled. When set to **NO** (default), banner display is according to the check box selection in the *Banners Configuration* dialog box.

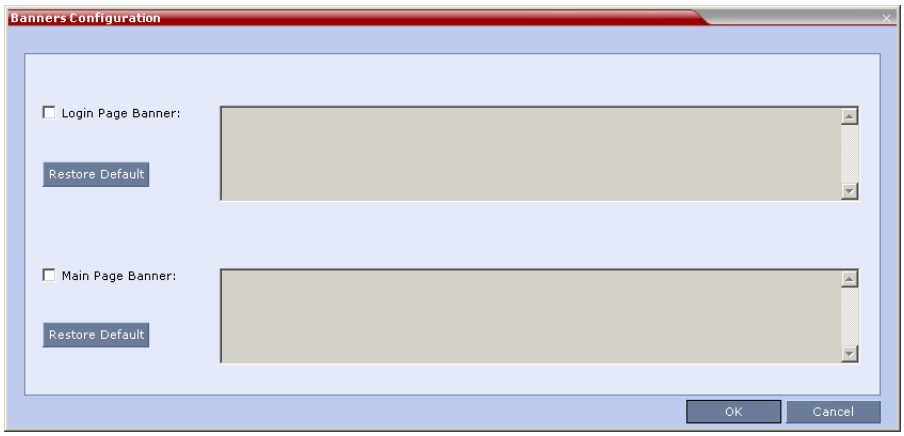
Customizing Banners

The *Login* and *Main Screen* banners can be customized to display conference information, assistance information or warning text as required in the *Enhanced Security Mode*.

To customize the banners:

1 In the RMX menu, click **Setup > Customize Display Settings > Banners Configuration**.

The *Banners Configuration* dialog box opens.



2 Customize the banners by modifying the following fields:

Table 7 *Banner Configuration*

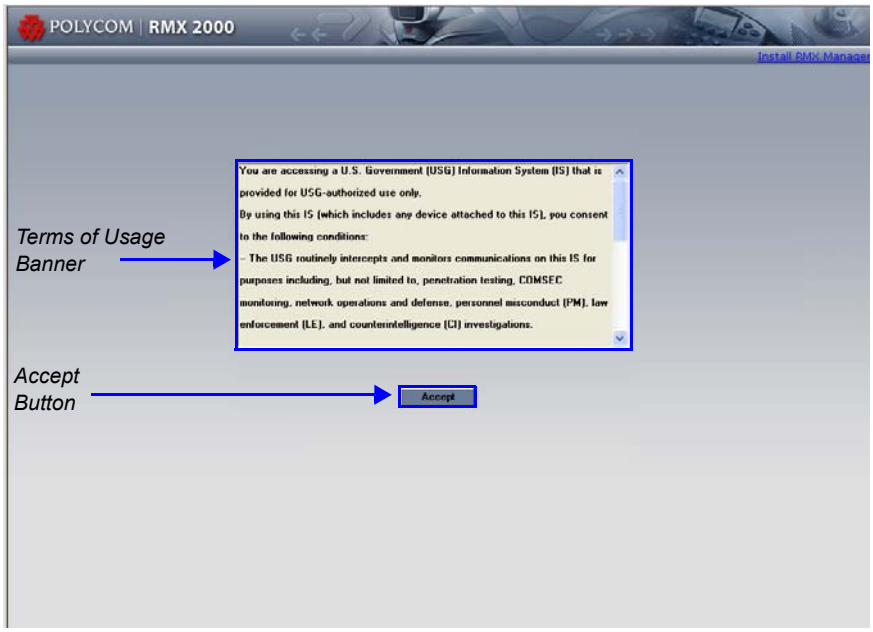
Field	Description		
	Check Box	Text Field	Restore Default Button
Login Page Banner	Select or clear the check box to enable or disable the display of the banner. **Note:** Banner display cannot be disabled in when the JITC_Mode flag is set to YES.	Edit the text in this field to meet local requirements: • Banner content is multilingual and uses Unicode, UTF-8 encoding. All text and special characters can be used. • Maximum banner size is 100KB. • The banner may not be left blank when the JITC_Mode flag is set to YES.	Click the button to restore the default text to the banner
Main Page Banner			

3 Click the **OK** button.

Banner Display

Login Screen Banner

The *Login* screen banner can display any text, for example the terms and conditions for system usage (default text) that is required in the *Enhanced Security Mode*. The RMX User must acknowledge that the information was read and click the **Accept** button to proceed to the *Login* screen as shown in the following screen:


POLYCOM | RMX 2000
Install RMX Manager
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
Terms of Usage Banner
Accept Button
Accept

When the RMX is configured to work in *Enhanced Security Mode*, the display banner includes the terms and conditions for system usage as detailed in the default text:

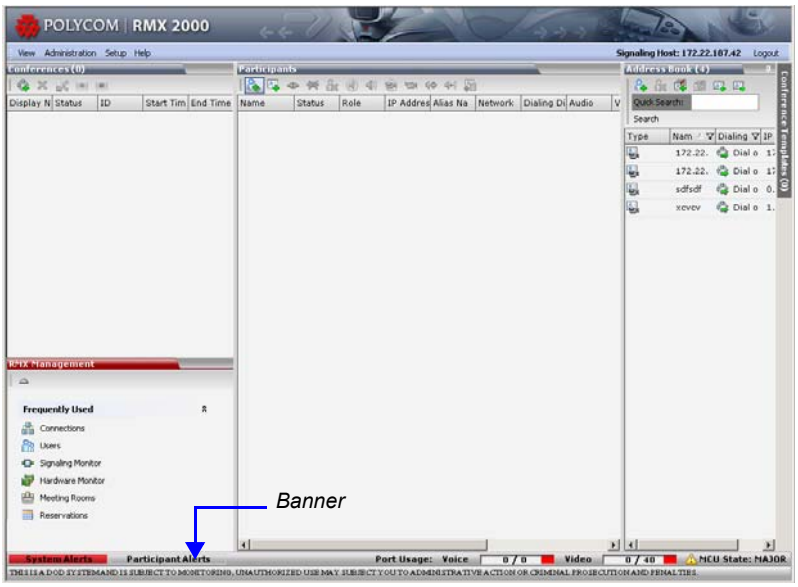
```
You are accessing a U.S. Government (USG) Information System (IS)
that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS),
you consent to the following conditions:
```

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Main Screen Banner

The *Main Screen* banner is displayed at the bottom of the screen, as follows:



When the RMX is configured to work in *Enhanced Security Mode*, the display banner includes the following default text:

```
THIS IS A DOD SYSTEM AND IS SUBJECT TO MONITORING, UNAUTHORIZED USE
MAY SUBJECT YOU TO ADMINISTRATIVE ACTION OR CRIMINAL PROSECUTION AND
PENALTIES.
```

Users Management

Additional security measures can be implemented in the RMX system by setting the appropriate system flags. These measures control the system users, the user connections to the RMX and the user login process.

Managing RMX users includes:

- User types that are not supported when the Enhanced Security Mode (JITC_MODE=YES) is enable.
- Disabling and enabling RMX Users
- Renaming RMX Users
- Disabling inactive users

Managing the user login process includes:

- Implementing Strong Passwords
- Implementing password re-use / history rules
- Defining password aging rules
- Defining password change frequency
- Forcing password change
- Conference and Chairman Passwords
- Locking out User
- Displaying the User Login record

Controlling the user sessions includes:

- Limiting the maximum number of concurrent user sessions
- User session timeout
- Limiting the maximum number of users that can connect to the system

Managing the RMX Users

When the RMX is configured to *Enhanced Security Mode (*the **JITC_MODE** *System Flag is set to* **YES)**, the following user management rules are automatically enforced:

User Types

- Auditor and chairperson user types are not supported.
- The *SUPPORT* user type is not allowed. If it exists, this user type is removed when the **JITC_MODE** *System Flag is set to* **YES** and the system is restarted.

The *Audit* files can be retrieved by the Administrator User.

Disabling/Enabling Users

- An administrator can disable a user or enable a disabled user, including administrators.
- The last administrator cannot be disabled.

For more information see "*Disabling, Enabling and Renaming Users*" on page **74**.

Renaming Users

- An administrator can rename any user, including administrators.
- A renamed user is considered by the system to be a new user and is forced to change his/her password.

For more information see "*Disabling, Enabling and Renaming Users*" on page **74**.

Disabling Inactive Users

Users can be automatically disabled by the system when they do not log into the RMX application for a predefined period. When the RMX is configured to *Enhanced Security Mode (*the **JITC_MODE** *System Flag is set to* **YES)**, this option is enforced.

- To enable this option, the **DISABLE_INACTIVE_USER** *System Flag* to a value between **1 to 90**. This value determines the number of consecutive days a user can be inactive before being disabled.

  When flag value is set to **0** (default in standard security environment), this option is disabled.

  The flag value is automatically set to **30** days when the **JITC_MODE** *System Flag is set to* **YES.**
- The user is marked as disabled but is not deleted from the system administrator/ operator database.
- The user remains disabled until re-enabled by an administrator.
- If a disabled user attempts to *Login*, an error message, *Account is disabled*, is displayed.
- The last remaining administrator cannot be disabled.

For more information see "*Disabling, Enabling and Renaming Users*" on page **74**.

Managing the User Login Process

Implementing Strong Passwords

Strong Passwords can be implemented for logging into the RMX management applications. They can be implemented when the system is in standard security mode or when in enhanced security mode.

The **FORCE_STRONG_PASSWORD_POLICY** *System Flag,* which enables or disables all password related flags cannot be set to **NO** and all *Strong Passwords* rules are automatically enabled and cannot be disabled when the **JITC_MODE** *System Flag* is set to **YES**.

If an administrator modifies any of the *Strong Passwords* flag settings, all users are forced to perform the password change procedure, ensuring that all user passwords conform to the modified *Strong Passwords* settings.

Administrators can change passwords for users and other administrators. When changing passwords for him/herself, other administrators or other users, the administrator is required to enter his/her own administrator's password.

Strong Passwords rules are enforced according to the settings of the various *Strong Passwords* flags as described in Table 5 on page **59**. Default settings of these flag change according to the system security mode.

Password Character Composition

- A *Strong Password* must contain **at least two** of **all** of the following character types:
  - Upper case letters
  - Lower case letters
  - Numbers
  - Special characters: @ # $ % ^ & * ( ) _ - = + | } { : " \ ] [; / ? > < , . (space) ~
- Passwords cannot contain the *User ID* (*User Name*) in any form. **Example:** A user with a *User ID*, *ben,* is not permitted to use "123**BeN**321" as a password because *BeN* is similar to the *User ID*.
- Passwords cannot contain more than four digits in succession.

When the strong password option is enabled and the password does not meet the Strong Password requirements an error, *Password characteristics do not comply with Enhance Security requirements,* is displayed.

Password Length

The length of passwords is determined by the value of the **MIN_PASSWORD_LENGTH** *System Flag*.

- Possible flag values are between 0 and 20.
- A *System Flag* value of **0** means this rule is not enforced, however this rule cannot be disabled when the *RMX* is in *Enhanced Security Mode*.
- In *Enhanced Security Mode,* passwords must be at least 15 characters in length (default) and can be up to 20 characters in length.
- If the *MIN_PASSWORD_LENGTH* flag is enabled and the password does not meet the required length an error, *Password is too shor*t, is displayed.

If the minimum password length is increased, valid pre-existing passwords remain valid until users are forced to change their passwords.

Implementing Password Re-Use / History Rules

Users are prevented from re-using previous passwords by keeping a list of previous passwords. If a password is recorded in the list, it cannot be re-used. The list is cyclic, with the most recently recorded password causing the deletion of the oldest recorded password.

- The number of passwords that are recorded is determined by the value of the **PASSWORD_HISTORY_SIZE** *System Flag*. Possible values are between 0 and 16.
- A flag value of **0** means the rule is not enforced, however this rule cannot be disabled when the *RMX* is in *Enhanced Security Mode*.
- In *Enhanced Security Mode,* at least 10 passwords (default) and up to 16 passwords must be retained.

If the password does not meet this requirement, an error, *New password was used recently*, is displayed.

Defining Password Aging

The duration of password validity is determined by the value of the **PASSWORD_EXPIRATION_DAYS** *System Flag*.

- Passwords can be set to be valid for durations of between 0 and 90 days.
- If the *System Flag* is set to **0**, user passwords do not expire. The *System Flag* cannot be set to **0** when the *RMX* is in *Enhanced Security Mode*.
- In *Enhanced Security Mode,* the minimum duration can be set to 7 days and the default duration is 60 days.

The display of a warning to the user of the number of days until password expiration is determined by the value of the **PASSWORD_EXPIRATION_WARNING_DAYS** *System Flag*.

- Possible number of days to display expiry warnings is between 0 and 14.
- If the *System Flag* is set to **0**, password expiry warnings are not displayed. The *System Flag* cannot be set to **0** when the *RMX* is in *Enhanced Security Mode*.
- In *Enhanced Security Mode,* the earliest warning can be displayed 14 days before passwords are due to expire and the latest warning can be displayed 7 days before passwords are due to expire (default setting).
- If a user attempts to log in after his/her password has expired, an error is displayed: *User must change password*.

Defining Password Change Frequency

The frequency with which a user can change a password is determined by the value of the **MIN_PWD_CHANGE_FREQUENCY_IN_DAYS** *System Flag*. The value of the flag is the number of days that users must retain a password.

- Possible retention period is between 0 and 7 days. In *Enhanced Security Mode* the retention period is between 1 (default) and 7.
- If the *System Flag* is set to **0**, users do not have to change their passwords. The *System Flag* cannot be set to **0** when the *RMX* is in *Enhanced Security Mode*.
- If a user attempts to change a password within the time period specified by this flag, an error, *Password change is not allowed before defined min time has passed*, is displayed.

An administrator can assign a new password to a user at any time.

Forcing Password Change

When the system is in *Enhanced Security Mode* the user is forced to change his/her password as follows:

- After modifying the value of the **JITC_MODE** *System Flag* to **YES**, all *RMX* users are forced to change their *Login* passwords.
- When an administrator creates a new user, the user is forced to change his/her password on first *Login*.
- If an administrator changes a users *User ID* name, that user is forced to change his/her password on his/her next *Login*.
- If a user logs in using his/her old or default password, the *Login* attempt will fail. An error, *User must change password*, is displayed.
- Changes made by the administrator to any of the *Strong Password* enforcement *System Flags* render users' passwords invalid.

Example: A user is logged in with a fifteen character password. The administrator changes the value of the **MIN_PASSWORD_LENGTH** *System Flag* to **20**.
The next time the user tries to log in, he/she is forced to change his/her password to meet the updated *Strong Password* requirements.

Managing Conference and Chairperson Passwords

The lengths of the Conference and Chairperson passwords are determined by the values of the **NUMERIC_CONF_PASS_MIN_LEN** and **NUMERIC_CHAIR_PASS_MIN_LEN** *System Flags*.

- Possible flag values are between 0 and 16.
- A *System Flag* value of **0** means these rules are not enforced, however these rules cannot be disabled when the *RMX* is in *Enhanced Security Mode*.
- In *Enhanced Security Mode,* Conference and Chairperson passwords must be at least 9 characters in length (default) and can be up to 16 characters in length.
- If the password does not meet these requirements an error, *Password is too shor*t, is displayed.

If the minimum password length is increased, valid pre-existing Conference and Chairperson passwords remain valid.

Hiding Conference and Chairperson Passwords

Conference and Chairperson Passwords that are displayed in the *RMX Web Client* or *RMX Manager* can be hidden when viewing the properties of the conference. When the value of the **HIDE_CONFERENCE_PASSWORD** *System Flag* is set to **YES,** these passwords are replaced by asterisks in the *RMX Web Client*, *RMX Manager*, *Audit Event* and *Log* files.

Temporary User Lockout

When the **JITC_MODE** *System Flag* is set to **YES,** *Temporary User Lockout* is implemented as a defense against *Denial of Service Attacks* or *Brutal Attacks*. Such attacks usually take the form of automated rapid *Login* attempts with the aim of gaining access to or rendering the target system (any network entity) unable to respond to users.

If a user tries to log in to the system and the *Login* is unsuccessful, the user's next *Login* attempt only receives a response from the *RMX* after 4 seconds.

User Lockout

User Lockout can be enabled to lock a user out of the system after three consecutive *Login* failures with same *User Name*. The user is disabled and only the administrator can enable the user within the system. User Lockout is enabled when the **USER_LOCKOUT** *System Flag* is set to **YES**.

If the user tries to login while the account is locked, an error message, *Account is disabled*, is displayed.

User Lockout is an *Audit Event*.

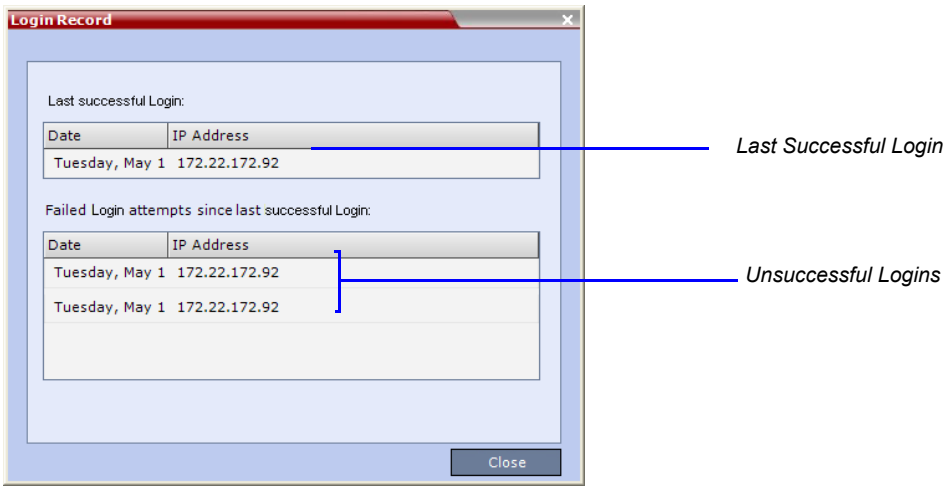
A system reset does not reset the *Login* attempts counter.

The time period during which the three consecutive *Login* failures occur is determined by the value of the **USER_LOCKOUT_WINDOW_IN_MINUTES** *System Flag*. A flag value of **0** means that three consecutive *Login* failures in any time period will result in *User Lockout*.

The duration of the *Lockout* of the user is determined by the value of the **USER_LOCKOUT_DURATION_IN_MINUTES** *System Flag*. A flag value of **0** means permanent *User Lockout* until the administrator re-enables the user within the system.

User Login Record

The system can display a record of the last *Login* of the user. It is displayed in the *Main Screen* of the *RMX Web Client* or *RMX Manager*. The user *Login Record* display is enabled when the **LAST_LOGIN _ATTEMPTS** *System Flag* is set to **YES**.



Both lists display the:

- *Date* and *Time* of the *Login* attempt.
- *IP Address* of the workstation initiating the *Login* attempt.

The list of unsuccessful *Logins* can contain up to ten records.

Failed *Login* attempts are written to the system *Log Files* and are recorded as *Audit Events*. The *Audit* files can be retrieved by the Administrator User.

Controlling RMX User Sessions

Management Sessions per System

It is possible for a several users to simultaneously log in to the *RMX* and initiate management sessions from different instances of the *RMX Web Client* or *RMX Manager* that are running on a single or several workstations.

The maximum number of concurrent management sessions (http and https connections) per system is determined by the value of the **MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM** *System Flag*.

Any attempt to exceed the maximum number of management sessions per system results in the display of an error message: *Maximum number of permitted user connections has been exceeded. New connection is denied.*

The log in attempt is recorded as an *Audit Event*

Sessions per User

It is possible for a user to log in to the *RMX* and initiate multiple management sessions from different instances of the *RMX Web Client* or *RMX Manager* that are running on a single or several workstations.

The maximum number of concurrent management sessions per user (http and https connections) is determined by the value of the **MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER** *System Flag*.

Any attempt to exceed the maximum number of management sessions per user results in the display of an error message: *A user with this name is already logged into the system. Additional connection is denied.*

The log in attempt is recorded as an *Audit Event*

Connection Timeout

If the connection is idle for longer than the number of seconds specified by the setting of the **APACHE_KEEP_ALIVE_TIMEOUT** *System Flag*, the connection to the *RMX* is terminated.

Session Timeout

If there is no input from the user or if the connection is idle for longer than the number of minutes specified by the setting of the **SESSION_TIMEOUT_IN_MINUTES** *System Flag*, the connection to the *RMX* is terminated.

A flag value of **0** means *Session Timeout* is disabled, however this feature cannot be disabled when the *RMX* is in *Enhanced Security Mode*.

Erase Session History After Logout

In *Enhanced Security Mode,* the *RMX Web Client* and *RMX Manager* leave no session information on the user's workstation or the MCU after the user logs off.

Cyclic File System Alarm

Cyclic Files

Cyclic files such as *Logger*, *CDR* and *Audit Event* files were automatically deleted by the system (oldest first) when the maximum number of files were reached. The deleted oldest files were replaced by a new current file.

The following table summarizes the maximum number of files per file type and RMX system type:

Table 8 *Cyclic Files by RMX System Type*

File Type	RMX 2000	RMX 4000
Log	4000	8000
CDR	2000	4000
Audit	1000	1000

In Version 4.5.0.F the RMX displays Active Alarms before overwriting the older files, enabling the users to backup the older files before they are deleted.

The display of Active Alarms is controlled by the **ENABLE_CYCLIC_FILE_SYSTEM_ALARMS** *System Flag*.

If the *ENABLE_CYCLIC_FILE_SYSTEM_ALARMS* is set to **YES** (default setting when **JITC_MODE** *System Flag* is set to YES) and a *Cyclic File* reaches a file retention time or file storage capacity limit, one of the following an *Active Alarms* is created:

- Backup of Log files is required
- Backup of CDR files is required
- Backup of Audit files is required

The administrator must use the relevant utility (*Logger*, *CDR*, *Auditor*) to retrieve and back up the indicated old file.

File retrieval information is contained in the file name.

Example:

- An old *Audit Event* file that has not been retrieved and backed up has a file name as follows:
  `Audit_SN0000000056_FMD27112008_FMT081433_LMD27112008_LMT081746_SZ53921_SUY_CFnone_NFV02_RTN.xml`
  - The **RTN** at the end of the filename indicates that the file has not been retrieved.
- An old *Audit Event* file that has been retrieved and backed up has a file name as follows:
  `Audit_SN0000000056_FMD27112008_FMT081433_LMD27112008_LMT081746_SZ53921_SUY_CFnone_NFV02_RTY.xml`
  - The **RTY** at the end of the file name indicates that the file has been retrieved.

Although the *Active Alarm* is cleared when the old file is retrieved, it is the administrator's responsibility to back up the file.

Restricting Content Broadcast to Lecturer

Content broadcasting can be restricted to the conference lecturer only, when one of the conference participants is set as the lecturer (and not automatically selected by the system). Restricting the Content Broadcast prevents the accidental interruption or termination of H.239 Content that is being shared in a conference.

Content Broadcast restriction is enabled by setting the **RESTRICT_CONTENT_BROADCAST_TO_LECTURER** *system flag* to **ON**. When set to OFF (default) it enables all users to send Content.

When enabled, the following rules apply:

- Content can only be sent by the designated lecturer. When any other participant tries to send Content, the request is rejected.
- If the RMX user changes the designated lecturer (in the *Conference Properties - Video Settings* dialog box), the Content of the current lecturer is stopped immediately and cannot be renewed.
- The RMX User can abort the H.239 Session of the lecturer.
- Content Broadcasting is not implemented in conferences that do not include a designated lecturer and the lecturer is automatically selected by the system (for example, in *Presentation Mode*).

Version 4.5.0.F Detailed Description - Changes to Existing Features

User Management

Disabling, Enabling and Renaming Users

Disabling a User

An administrator can:

- Disable an enabled user
- Enable a disabled user

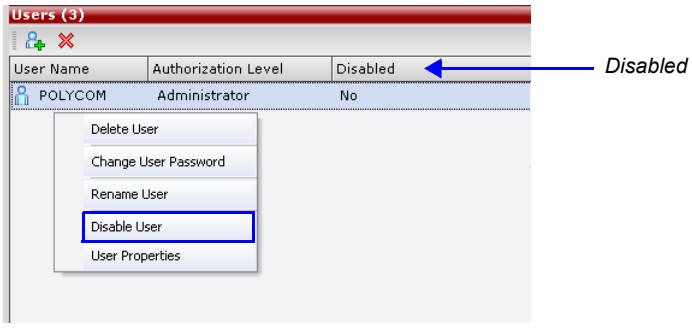
An additional field, *Disabled*, has been added to the *Users* pane in both the *RMX Web Client* and *RMX Manager* to support this feature.

To disable a user:

1 In the *RMX Management* pane, click the **Users** ( ) button.

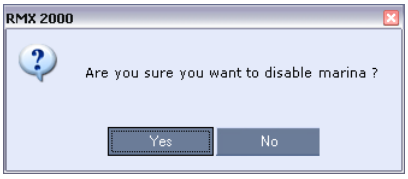
The Users pane is displayed.

2 In the *Users* pane, right-click the user to be disabled.



3 Select **Disable User** in the menu.

A confirmation box is displayed.



4 Click **YES**.

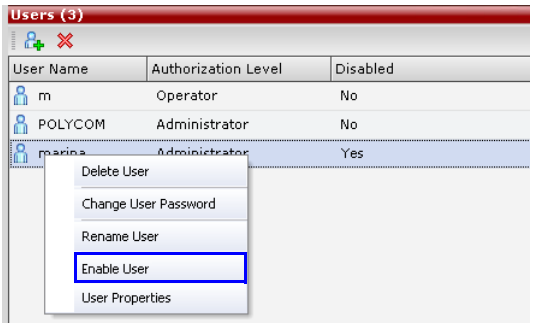
Enabling a User

To enable a user:

1 In the *RMX Management* pane, click the **Users** ( ) button.

The *Users* pane is displayed.

2 Right-click the user to be enabled and select **Enable User**.



A confirmation box is displayed.

3 Click **YES**.
The User status in the *Users* list - *Disabled* column changes to **NO**.

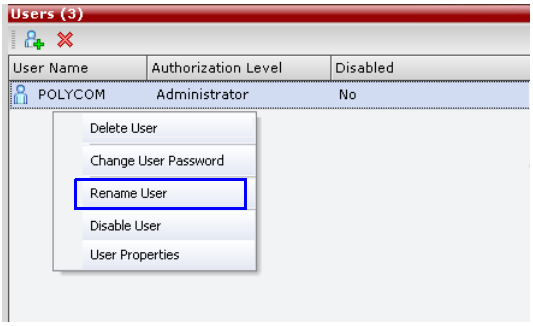
Renaming a User

To rename a user:

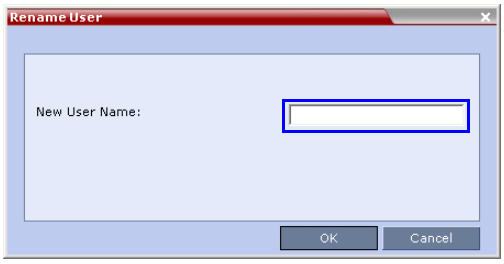
1 In the *RMX Management* pane, click the **Users** ( ) button.

The Users pane is displayed.

2 Right-click the user to be renamed and select **Rename User**.



The *Rename User* dialog box is displayed.



3 Enter the user's new name in the *New User Name* field and click **OK**.

The user is renamed and is forced to change his/her password.

Software Management

System Backup and Restore

In all previous versions the *Backup Configuration* and *Restore Configuration* operations collected the various configuration files by directly accessing the file system of the *RMX*. This version does not permit direct access to the *RMX* file system.

Backup and Restore Guidelines

- Direct access to the *RMX* file system is disabled in both *JITC Mode* and non *JITC Mode*.
- *System Backup* can only be performed by an administrator.
- The *System Backup* procedure creates a single backup file that can be viewed or modified only by developers.
- A *System Backup* file from one system can be restored on another system.
- To ensure file system consistency, all configuration changes are suspended during the backup procedure.
- The following parameters, settings and files are backed up:
  - MCMS configuration files (/mcms/Cfg):
  - Network and service configurations,
  - Rooms,
  - Profiles
  - Reservations
  - System Flags
  - Resource Allocation
  - IVR messages, music
  - RMX Web Client user setting - fonts, windows
  - RMX Web Client global settings – notes, address book, language
  - Private keys and certificates (TLS)
  - Conference participant settings
  - Operation DB (administrator list)
  - SNMP settings
  - Time configuration

Installing RMX Manager for Secure Communication Mode

The *RMX Manager* cannot be downloaded from a site, operating in *Secure Communication Mode*, without a valid TLS certificate.

The following procedure describes how to obtain a TLS certificate and download the *RMX Manager* from a site operating in *Secure Communication Mode*.

FIPS is always enabled in Enhanced Security Mode, and when ClickOnce is used to install RMX Manager, the workstation must have one of the following installed:

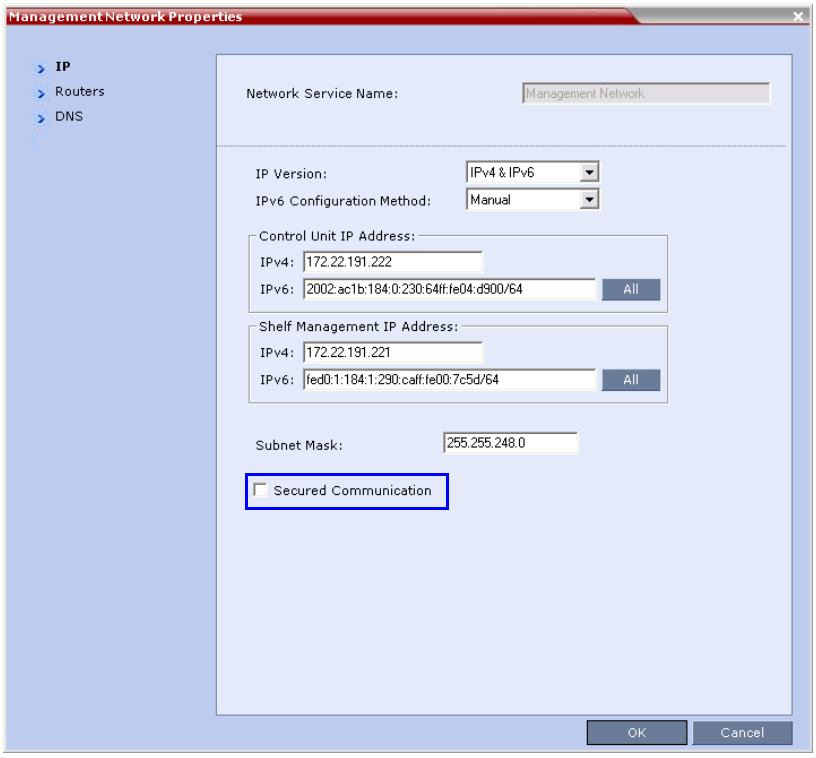
- *.NET Framework 3.5* or a later version of the *.NET Framework.*
- *.NET Framework 2.0* plus *Service Pack 1* or later.

1 Set the *RMX* to *Non Secure Communication Mode*

a In the *RMX Management* pane, click **IP Network Services.**

b In the *IP Network Services* list pane, double click the **Management Network** entry.

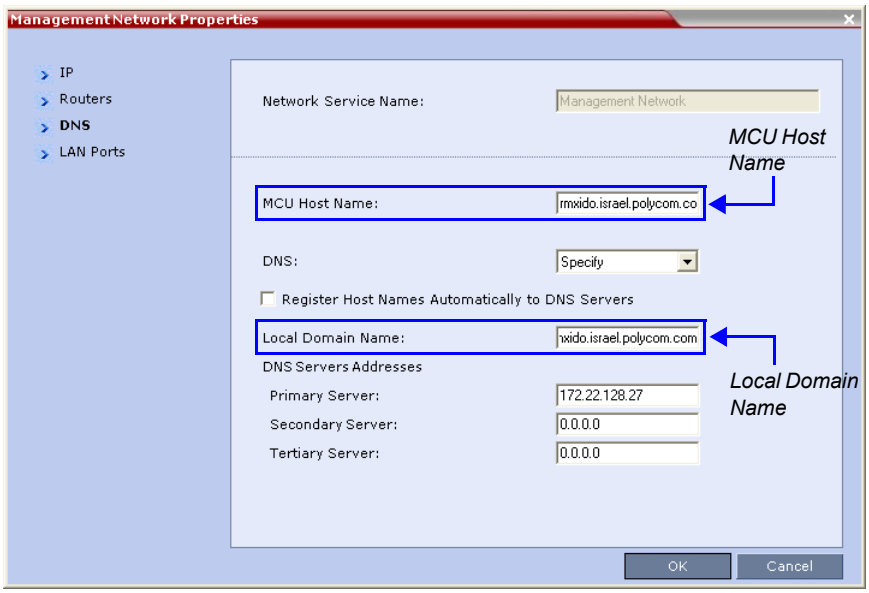
The *Management Network Properties* dialog box is displayed.



c Clear the *Secured RMX Communication* check box.

d Click **OK**.

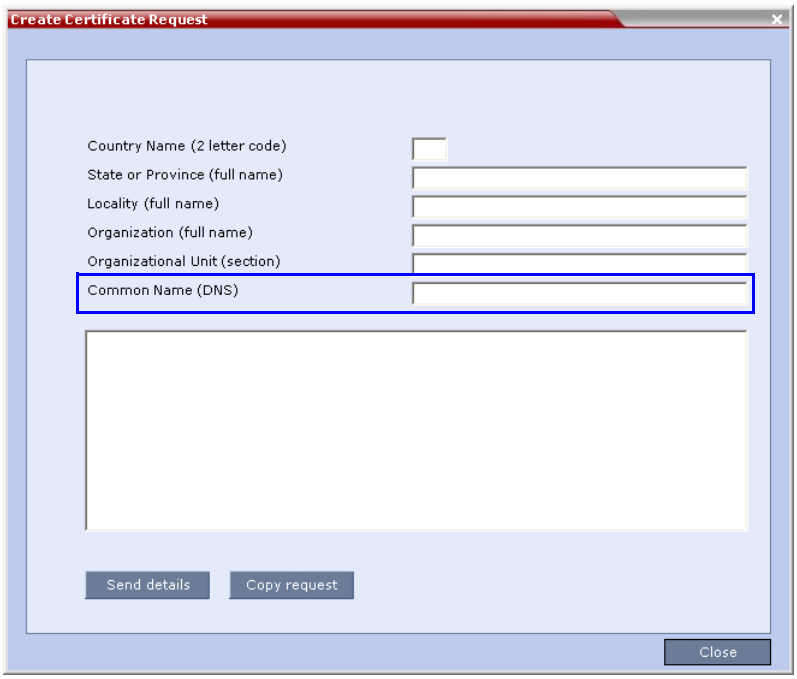
2 Click the **DNS** tab.



3 Enter the *Local Domain Name*.

The *Local Domain Name* must be the same as the *MCU Host Name*. If the content of these two fields are not identical an active alarm is created.

4 Create a *Certificate Request*.

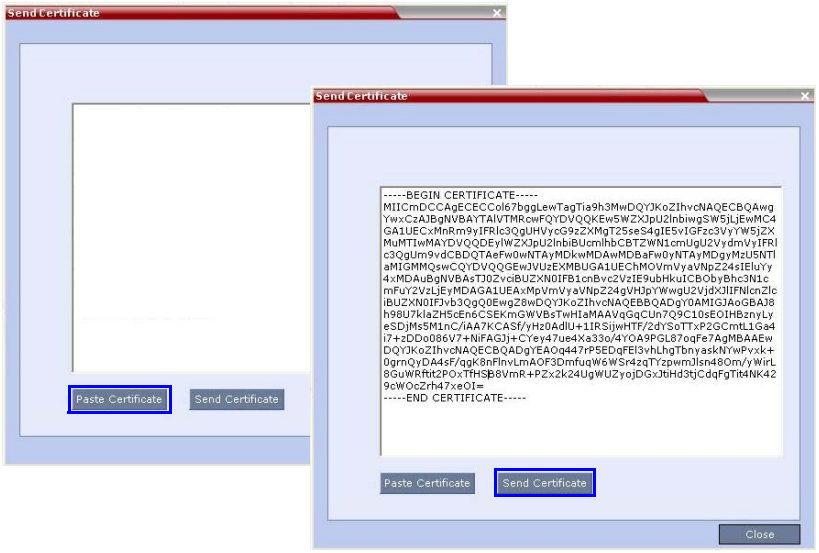


The *Common Name (DNS)* must be the same as the *MCU Host Name* configured in the *Management Network Properties* dialog box.

For more information, see the *RMX 2000/4000 Administrator's Guide, RMX 2000/4000 Administrator's Guide for Maximum Security Environments*, "*Secure Communication Mode*" on page **F-1**.

Certificates can also be created and issued using an *Internal Certificate Authority*. For more information see "*Using an Internal Certificate Authority*" on page **80**.

5 Install the certificate.



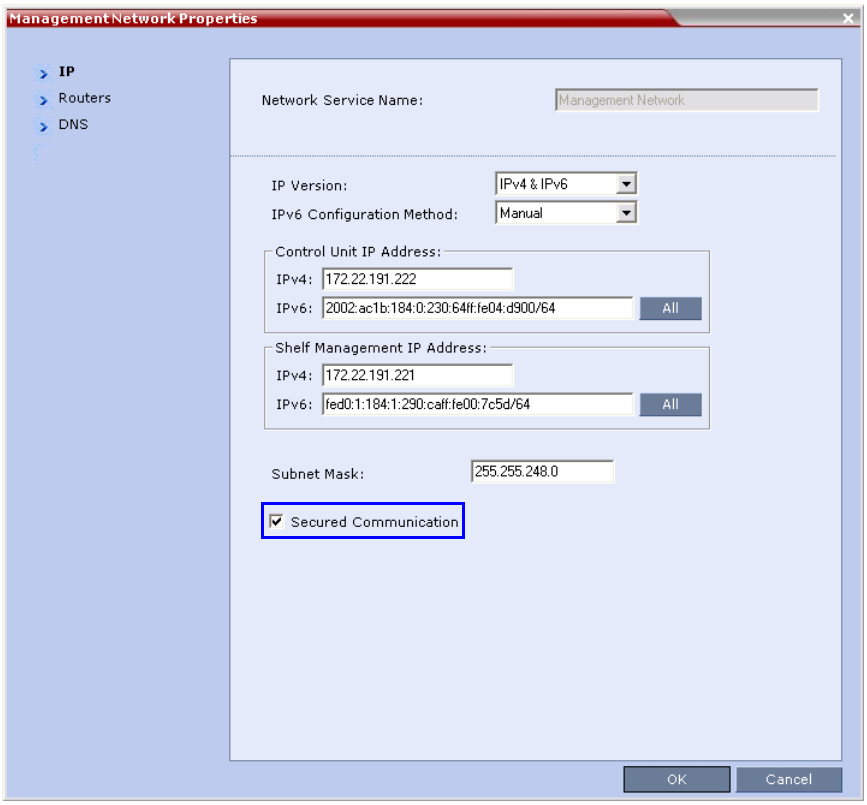
For more information, see the *RMX 2000/4000 Administrator's Guide, RMX 2000/4000 Administrator's Guide for Maximum Security Environments*, "*Secure Communication Mode*" on page **F-1**.

6 Set the *RMX* to *Secure Communication Mode*.

7 Set the *RMX* to *Secure Communication Mode*

- **a** In the *RMX Management* pane, click **IP Network Services.**
- **b** In the *IP Network Services* list pane, double click the **Management Network** entry.

The *Management Network Properties* dialog box is displayed.



c Select the *Secured RMX Communication* check box.

d Click **OK**.

8 Reset the *RMX*:

a In the *RMX Management* pane, click the **Hardware Monitor button**.

The *Hardware Monitor* pane is displayed.

b Click the **Reset** ( ) button.

9 Install the *RMX Manager*. For more information, see the *RMX 2000/4000 Administrator's Guide for Maximum Security Environments*, "*Installing RMX Manager for Secure Communication Mode*" on page **14-1**.

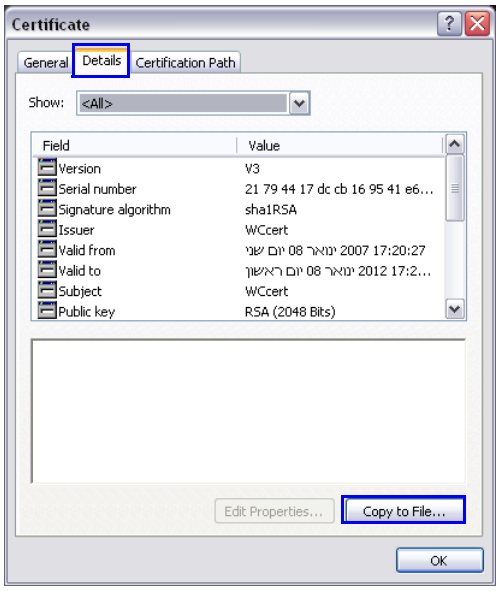
Using an Internal Certificate Authority

If your TLS certificate was created and issued by an *Internal Certificate Authority*, it may not be seen as having been issued by a trusted *Certificate Authority*. The *RMX Manager* is not downloaded successfully and a warning is received stating that the certificate was not issued by a trusted *Certificate Authority*.

To add the Internal Certificate Authority as a trusted Certificate Authority:

1 Navigate to the folder where the certificate (.cer) file is saved.

2 Open the certificate file.



3 Click the **Detail** tab.

4 Click the **Copy to File** button.

The *Certificate Export Wizard* is displayed.

Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

5 Click the **Next** button.

The *Export File Format* dialog box is displayed.

Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
Delete the private key if the export is successful
< Back
Next >
Cancel

6 Select **Base-64 encoded X.509 (.CER)**.

7 Click the **Next** button.

The *File to Export* dialog box is displayed.

8 In the *File Name* field, enter the file name for the exported certificate.

9 Click the **Next** button.

The final *Certificate Export Wizard* dialog box is displayed.

10 Click the **Finish** button.

The successful export message is displayed.

11 Click the **OK** button.

Additional Auditor Features and Events

The *Event Auditor* can assess CDR log files.

The following additional *Auditor Events* are reported by the *Shelf Management* module:

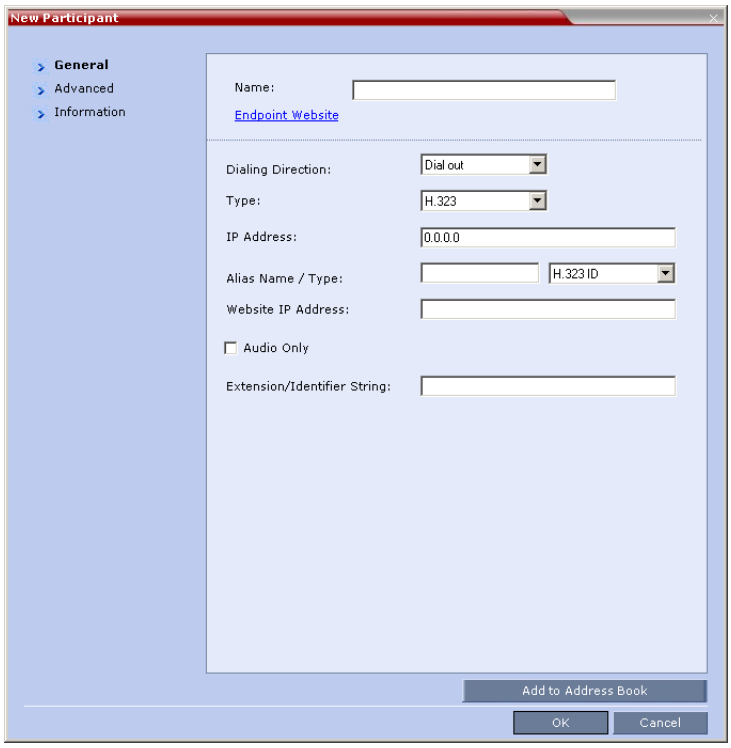
- Login
- Failed login attempt
- Logout
- Session disconnected without logout due user closing the browser, TCP disconnection etc.
- Management Session Time Out as a result of the session being idle for the time specified by the value of the **SESSION_TIMEOUT_IN_MINUTES** *System Flag*.
- Attempt to exceed the maximum number of management sessions per system as specified by the value of the **MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM** *System Flag.*
- Attempt to exceed the maximum number of management session per user as specified by the value of the **MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER** *System Flag*.
- All System Resets.
- *USB key* used to change system configuration.

Dial-out Extension/Identifier String

Dial-out participants that connect to an external device such as *Cascaded Links* or *Recording Links* may be required to enter a conference password or an identifying string to connect. A new field that was added to the *Participant Properties - General* dialog box enables the RMX to automatically send this information upon connection to the destination device/conference. The information is sent by the RMX as DTMF code to the destination device/conference, simulating the standard IVR procedure.

To add the Extension/Identifier String Information:

1 In the *Participant Properties - General* dialog box, define the required participant information.



2 In the *Extension/Identification String* field, enter the required string as follows:

[p]…[p][string]
For example: pp4566#

- **p - optional** - indicates a pause of one second before sending the DTMF string. Enter several concatenated [p] to increase the delay before sending the string. The required delay depends on the configuration of the external device or conference IVR system.
- **String** - enter the required string using the digits 0-9 and the characters * and #. The maximum number of characters that can be entered is identical to the H.323 alias length.

If the information required to access the device/conference is composed of several strings, for example, the conference ID and the conference password, this information can be entered as one string, where pauses [p] are added between the strings for the required delays, as follows:

[p]…[p][string][p]…[p] [string]..
For example: **p23pp*34p4566#**

New CDR Events

New events were added to the CDR:

- RESERVED_PARTICIPANT_CONTINUE_IPV6_ADDRESS (2011)
- USER_ADD_PARTICIPANT_CONTINUE_IPV6_ADDRESS (2102)
- USER_UPDATE_PARTICIPANT_CONTINUE_IPV6_ADDRESS (2106)
- EVENT_NEW_UNDEFINED_PARTY_CONTINUE_IPV6_ADDRESS (32)

Table 9 *Event Fields for Events 2011, 2102, 2106 and 32*

Field	Description
IP V6	IPv6 address of the participant's endpoint.

New Active Alarms

The following Active Alarms were added to the system:

Table 10 *New Active Alarms in Version 4.5.0.F*

Active Alarm	Description
Alarm generated by a Central Signaling component	A system alert was generated by a component of the Central Signaling.
Alarm generated by an internal component	A system alert was generated by an internal system component.
Product Type mismatch. System is restarting.	The user is alerted to a mismatch between the product type that is stored in MCU software and the product type received from another system component. In such a case the system is automatically restarted.
CPU slot ID not identified	The CPU slot ID required for Ethernet Settings was not provided by the Shelf Management.
The system has been configured for JITC mode, but communication is not secured until a TLS certificate is installed and the MCU is set to Secured Communication.	Although the System Flag JITC_MODE is set to YES, the Enhanced Security Mode is not fully implemented as the TLS certificate was not installed. Please install the TLS certificate and set the MCU to Secured Communication Mode to fully enable the Enhanced Security Environment.
Backup of CDR files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when JITC_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that CDR files need to be backed up.
Card failed to switch to Enhanced Security Mode	Card failure occurred when the system was set to Enhance Security Mode (JITC_MODE=YES).
Backup of log files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when JITC_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that log files need to be backed up.
Backup of audit files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when JITC_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that audit files need to be backed up.
GUI System configuration file is invalid XML file	The XML format of the system configuration file that contains the user interface settings is invalid.

Table 10 *New Active Alarms in Version 4.5.0.F*

Active Alarm	Description
Bios version is not compatible with Enhanced Security Mode.	The current BIOS version is not compatible with Enhanced Security Mode (JITC_MODE=YES).
User Name "SUPPORT" cannot be used in Enhanced Security Mode	When Enhanced Security Mode (JITC_MODE=YES) is enabled, the User Name "SUPPORT" cannot be used to define a new User.
Restore Succeeded	Restoring the system configuration has succeeded. Reset the MCU.
Restore Failed	Restoring the system configuration has failed as the system could not locate the configuration file in the selected path, or could not open the file.
Encryption Server Error. Failed to generate the encryption key	FIPS 140 test failed while generating the new encryption key.

Corrections and Known Limitations

Corrections Between Version 4.5.0.F and Version 5.1.0.G

Table 11 Corrections Between Version 4.5.0.F and Version 5.1.0.G

No.	Category	Description	ID/ VNGR#
1	Cascade	Site names are displayed incorrectly when connecting endpoints to a cascaded conference that is already connected by the cascaded link.	12753 VNGFE-2278
2	Content	In a 768 Kbps conference with Content & H.264, HDX and VSX endpoints video rates were not increased after Content was terminated in the conference.	12225
3	Encryption	H.320 FX endpoint does not connect to the conference when encryption is turned on.	12212
4	Gateway	When an IP participant dials the Gateway Profile on RMX A and enter a destination conference ID of a conference running on RMX B, the participant connects correctly to the second RMX but the site name displays the name of RMX A instead of the endpoint name.	13334/ 12881 VNGFE-2377
5	General	RMX is showing “Overflow in /output” as the hard drive is not recognized by the controller.	13607/ VNGFE-2497
6	General	*Restore Factory Defaults* dialog box is translated incorrectly in Japanese.	12690/ VNGBE-810
7	General	When connecting to RMX 4000, default MCU *Display Name* is POLYCOM RMX 2000 instead of RMX 4000.	12689/ VNGBE-811
8	General	Sometimes, endpoints fail to connect to a conference after modifying the Profile assigned to that conference and a major alert “Power off” is displayed.	12618/ VNGBE-784
9	General	When logged in to RMX Web Client in Japanese and trying to download the software using A*dministration* > *Software Management* > *Software Download*, the *build.bin* file cannot be found.	12615/ VNGBE-782
10	General	When logged in to RMX Web Client in Japanese, the Telepresence value in Administration > System Information is displayed in English.	12518/ VNGBE-758

Table 11 Corrections Between Version 4.5.0.F and Version 5.1.0.G

No.	Category	Description	ID/ VNGR#
11	General	Incorrect Japanese translation of the error message displayed when creating an EQ and using a dial-in number already assigned to another conferencing entity.	12514/ VNGBE-773
12	General	In the Japanese RMX Web Client, the conference deletion message is displayed in English.	12453
13	General	When logged in to RMX Web Client in Japanese and opening a file in the Auditor Viewer (Administration > Tools > Auditor Viewer, click local file icon), the dialog box title that is show in Japanese switches to English after opening the file.	12447/ VNGBE-755
14	General	In the Japanese RMX Web Client, the New Reservation > Schedule > Monthly option has an incorrect translation.	12427
15	General	Rarely, a false active alarm appears: “Temperature has reached a problematic level and requires attention” for no apparent reason.	12059
16	General	When an RTM LAN card is changed on an activated system, a Power off error message is displayed for all the MPM+ cards on the system, although the MCU continues to work normally.	11970
17	General	RMX status changes to Major following RMX failure to connect to the NTP servers.	13266 VNGFE-2312
18	General	NTP failure message remained after “Socket reconnect (board id: 5)” procedure.	13247/ 13331 VNGFE-2336
19	General	Core dump occurs and endpoints cannot move from the EQ to the destination Ad Hoc conference created when: • The RMX is configured to Fixed Resource Capacity and all resources are set to CIF/VSW • The system flag ENABLE_H239=NO.	12712/ 12713/ 13332 VNGFE-2359
20	General	Insufficient resources indication and a Major alarm are displayed when the MPM card did not complete the startup process and could not be recognized by the system.	13335 VNGFE-2320
21	General	After the upgrade to v4.1.1.19, newly created Meeting Rooms cannot be used, but existing Meeting Rooms work successfully	13351 VNGFE-2452

Table 11 Corrections Between Version 4.5.0.F and Version 5.1.0.G

No.	Category	Description	ID/ VNGR#
22	General	Card recovery process does not work.	13185 VNGFE-2414
23	Interoperability	In a conference with a line rate of 1920Kpbs, LPR and AES enabled, H.320 Tandberg MXP dial-in participants cannot connect and an assert appears.	12069
24	Interoperability	When connecting a Tandberg MXP ISDN endpoint to an encrypted conference, loud buzzing noises occur.	11962
25	Interoperability	When an DMA Gateway places dial-in audio calls through an RMX Gateway (versions older than 4.1.1), the audio calls cannot connect at the destination RMX installed with Version 4.1.1.	11959
26	Interoperability	In a CP conference with a line rate of 384Kbps, when 2 HDX and one VSX endpoints are connected, the VSX receives bad video.	11609
27	Interoperability	Green artifacts appear when a LifeSize Room 200 endpoint connects to a HD Video Switching Meeting Room at a line rate of 1024Kbps.	13338/ VNGFE-2309
28	Interoperability	The video displayed on the VSX endpoint is distorted (stretched), when two endpoints (VSX 7000 and HDX 8000) remain in a conference that is set to Motion, Auto Layout at line rate of 512 Kbps and the video layout changes to 1x1.	13354 VNGFE-2411
29	Interoperability	After MCU reset performed from Hardware Monitor, no audio could be heard when participants were routed via DMA to a conference running on RMX 4000.	13194/ VNGFE-2406
30	Interoperability	No Content is sent or received by the ISDN endpoint when connecting through the RMX GW to a Virtual Room managed by the DMA (Version 4.1.1.1_Build_15_SP_2) running on the RMX.	13405/ VNGFE-2468
31	Interoperability	Polycom audio IP endpoints experience various problems when they attempt to call into DMA conferences.	13507/ DMA-385
32	Interoperability	Cannot dial out from a conference running on RMX 2000 Version 5.0 to Avaya 1XC (Version CM 5.2 and 6.0) and Polycom endpoints.	13632 AVA-1038

Table 11 Corrections Between Version 4.5.0.F and Version 5.1.0.G

No.	Category	Description	ID/ VNGR#
33	IP	Occasionally, problems are encountered with the Gatekeeper and memory. The process recovers seamlessly without effecting the overall experience.	12255
34	IP	Latency is always shown as 0 in the Participant's Connection Status.	11749 VNGFE-2241
35	ISDN/Gateway	Content is not sent from an IP HDX endpoint to an ISDN VSX endpoint via the RMX 2000 gateway when connecting at a line rate of 256 Kbps and the Gateway Profile is set to 'Motion'.	13561/ VNGFE-2489
36	ISDN	Occasionally, RMX with MPM cards and the audio/video slider is set to 180 audio has limited inbound audio only calls through ISDN to 46 participants. The 47th participant that connects hear a fast busy tone. This limitation is cleared when the system is reset.	13653/ VNGFE-2224
37	IVR	A conference with a 1920Kbps Line Rate and IVR Service that includes a Welcome Slide, both the Welcome Slide and Video are partially blacked out.	12021/ 12031
38	IVR	IVR Roll Call Tone is replaced by a recorded participant name due to overwriting the tone *.wav file by the recorded file.	12564 VNGFE-2350
39	Reservations	An error message is displayed when checking the properties of a reservation in the Calendar view for the first time and the ISDN/PSTN dial in option is disabled for the reservation.	11046 VNGFE-2286
40	Reservations	When an on-going conference duration is set to one minute and auto-extend enabled with an ISDN dial in number, the RMX may not detect an ISDN dial-in No. conflict when placing a reservation on the bridge with an identical ISDN number. In case of a dial-in number conflict, incoming calls are routed to the on-going conference and not to the reserved meeting.	11635
41	RMX Manager	Cannot install the RMX Manager application from RMX 4000.	12718/ VNGBE-727/ 825

Table 11 Corrections Between Version 4.5.0.F and Version 5.1.0.G

No.	Category	Description	ID/ VNGR#
42	RTM ISDN	During an ongoing conference, connection with the RTM ISDN card is lost, causing the ISDN participant to disconnect from the conference, and hardware reset was required to restore the connection with the card.	12975/ VNGFE-2378
43	SIP	Occasionally, when a dial-in SIP participant accesses the Entry Queue, the participant connection fails even though the participant entered the correct conference ID.	12017
44	SIP	When trying to connect SIP participant thru external API application, when the URI and IP address fields are switched (the IP address is left empty and the URI is set to the IP address), the endpoint will disconnect.	11971
45	SIP	The maximum number of Meeting Rooms, Entry Queues, SIP Factories and on-going conferences that can be registered to the Proxy, is limited to 100.	11949/11923
46	SIP	The error message “”Network does not have enough resources to complete your call. Try calling at a lower rate” is displayed when two SIP (CMAD) participants dial in to the conference at the same time.	13308
47	SIP	Cannot dial out to a SIP endpoint.	13384/ 13657 VNGFE-2450
48	Upgrade	After upgrading from Version 4.1.1.19 to Version 5.0, and the RMX was configured to work with CMA Address Book, the RMX Login window is not displayed.	13189/ VNGFE-2417
49	Video	Sometimes, the video processing units on the MPM cards are not responding and MCU reset is required.	13415/ VNGFE-2460

Corrections Between Version 4.1.1 and Version 5.0

Table 12 Corrections Between Version 4.1.1 and Version 5.0

No.	Category	Description	ID/ VNGR#
1	Interoperability	Some HDX endpoints connect at 4SIF resolution even if line rate is 1 Mb.	11697
2	Video	Site names are not displayed in 4x4 and 1+10 layouts.	11680
3	Content	Legacy endpoints do not return to conference layout after Content is stopped.	12342/ 2283
4	General	On a PC with Vista OS, the RMX Manager application cannot be installed.	12195
5	General	In the Hardware Monitoring, statistics are not displayed when monitoring the LAN	12298
6	General	A "$" in the password of an RMX Version 3.0 or 4.0 account prevents access to Hardware Monitor and generates an error when user tries to access the hardware	10341/ 1992
7	General	The Operator and Chairperson are able to delete a participant from the address book when they are not authorized to do so.	9930/ 9931
8	Interoperability	PictureTel Concorde 4500 ZX endpoint connects to a conference as Secondary (no video) when using ISDN and H.261 capabilities.	9721
9	Interoperability	Frozen Video on VSX6000 and V500 in CP session set to sharpness	11412
10	Interoperability	When endpoints connect to a conference running on the RMX through the DMA, the endpoints will see full screen (1x1) layout and not the conference layout.	11508
11	Interoperability	When using an RMX MCU and a Codian MCU together, each with one ISDN endpoint connected, the endpoint connected to the Codian MCU displays a horizontally stretched picture.	11753
12	Interoperability	Can't connect Sony PCS-1600s over ISDN	11672/ 2219
13	Interoperability	An Ipower v6.2.0.1208 endpoint connecting to an RMX with Siren 14 or G722.1 audio algorithm receives garbled / chopped audio.	11854/ 2258
14	Interoperability	RMX audio is muted or garbled when dialing from PVX endpoints to other endpoints, via the RMX.	11881/ 2277

Table 12 Corrections Between Version 4.1.1 and Version 5.0

No.	Category	Description	ID/ VNGR#
15	Interoperability	On an RMX 2000 (ver.3.xx) with an H.323i Power (ver. 6.2) endpoint connected at a 256Kbps line rate, the audio from iPower is garbled.	9396/ 1654
16	IP	After definition, the Static Route malfunctions.	12288
17	ISDN	No Voice Activated Switching when connecting to an ISDN Video participant	11392/ 2024
18	Partners - Microsoft	After the .pfx file is installed, the RMX has to be reset in order for it to register to the OCS server and to enable SIP calls. Initiate the Reset from the Hardware Monitor list as no prompt is displayed.	11516
19	Recording	Recording links on RMX 4.0 do not support AES encryption, although the RSS v4.0 and above have an AES encryption option	11664/ 2186
20	Resource Capacity	When the Resource Capacity Mode is set to Flexible and the Port Configuration slider is moved, an incorrect message displays requesting that the RMX be reset.	10884
21	Web Client	After logging-in and out several times in the Web Manager, the UI appears in English instead of French.	12096

Version 5.1.0.G System Limitations

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
1	Avaya Environment	An Avaya OneX SIP video endpoint places a point-to-point call to another Avaya OneX SIP video endpoint via the Avaya Communications Manager (ACM V5.2.0), and then another endpoint is added to the call. customer adds another endpoint. The first endpoint is placed on hold and a separate call is initiated. When they connect, the participant clicks on a button to create a conference. The ACM calls the RMX (v4.1.1.19) and creates an ad hoc conference on the RMX to create a multipoint call. The participant that initiated the call will partially connect.	VNGFE-2528	Setting the MAX_CP_RESOLUTION flag to CIF can solve this issue, however, it is not recommended as this will limit all video calls to CIF resolution.
2	Cascading	When connecting to a cascaded CP conference with a 768Kpbs line rate and the video quality set to Sharpness, HDX endpoints experience bad video quality.	11953	
3	CDR	When the conference termination time is changed, the CDR is not updated.	1569	
4		The Encryption field is missing from the CDR section.	3011	
5		When a conference was terminated by an MCU reset, an incorrect status “Ongoing Conference” will be displayed in the CDR List pane.	9340	
6		Wrong GMT Offset in RMX CDR	11691	
7		Wrong GMT Time Offset is written to the CDR.	11586, 11746, VNGBE-540	
8	CMA	When creating a conference using the CMA, the Conference Management UI displays the participants as disconnected, even though they are connected.	11543	
9	CMA	CMA does not support RMX4000 yet. Conference on Demand does not work.	12432	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
10	Content	Two conferences with 'Send Content To Legacy endpoints' function enabled, after moving a participant with an Legacy Endpoint the Content frame is partially blacked out for a few seconds.	11936	
11		Occasionally, when Content is send from an HDX endpoint, participants do not view Content.	12348	
12		In a conference with a line rate of 384Kbps, when H.323 participant connect to the conference using FECC, the Content channels do not open.	11470/ 11491	
13	Encryption	In an encrypted conference, Tandberg MXP endpoints encounter audio problems.	11401, 9568	
14		In an encrypted conference, H.323 encrypted dial-in and dial-out participants cannot connect and an assert appears.	12202	
15	Gateway	All endpoints that dial-in to a conference using a third party Gateway receive identical names in the RMX Manager Participant's pane.	1011	
16		When deleting the default Gateway Profiles and then opening a ISDN/PSTN Network Service, an error message appears.	10863	
17		When dialing from H.323 to ISDN using the *Gateway IVR* method and the string [Bridge prefix][GW profile], after entering the number of the destination ISDN endpoint, the connection indication on the endpoint screen pops up with each connection update.	10999	
18		When endpoint connects through MGC Gateway, the layout is automatically defined as a 1x1 'Personal' format instead of applying the conference layout.	12018	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
19	General	The *Click & View* menu doesn't appear in 64 Kbps calls.	3824	Use *RMX Web Client*.
20		When moving from MPM+ to MPM mode (with only MPM cards installed in the MCU), the *Card Configuration Mode*, indicated in the *System Information* dialog box, remains in MPM+ Mode.	9729	Logout and then login to the RMX Web Client.
21		When using the restore to factory defaults, after inserting the Activation key, the system requires a reset when the reset is not required.	9803	
22		After deleting an ISDN/PSTN Network Service, text that appears in the message alert is inconsistent.	10366	
23		When the Resource Capacity Mode is set to Flexible and the Port Configuration slider is moved, an incorrect message displays requesting that the RMX be reset.	10884	Ignore the message.
24		Dial out to participants assigned to a Meeting Room will only start when the dial-in participant who has activated it has completed the connection process and the Meeting Room has become an ongoing conference.	10922	
25		Mute incoming participants function (DTMF*86) is not applied to ISDN participants who dial in directly to the conference.	10967	When connecting via an Entry Queue Mute is applied.
26		When moving several participants using multiple selection from one conference to another conference whose maximum number of participants is exceeded by at least one of the moved participants, this participant cannot connect to the conference but is also disconnected from his/her source conference.	11064	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
27	General	When moving many participants simultaneously from one conference to the other (both with a line rate of 1920 Kbps), a number of HDX8000 endpoints connect secondary.	11324	Disconnect and reconnect the endpoints that are secondary.
28		Updating the Profile on a Conference Template is not applied when the conference becomes ongoing.	11383	
29		An assert fault “SOFTWARE_ASSERT_ FAILURE” sometimes appears when the RMX is running under load (repetitive connecting and disconnecting).	11701	
30		Participants sometimes do not connect when the RMX is running under load. The disconnection cause is stated as “MCU internal problem”.	11703	
31		When JITC_MODE flag is set to YES, a reset of the RMX is required after RMX Time is changed.	11714	
32		RMX Web Client users can drag participants to each other’s Operator conferences. Behavior is correct when using menu options: RMX Web Client users cannot drag participants to each other’s Operator conferences.	11741	
33		MCMS Version is listed as 0.0.0.0 in the Faults List Description field	11840	
34		When downloading a new activation key and clicking twice on the 'OK' button results in 'Invalid Key' message.	11987	Log out and login the web browser or reopen the internet explorer.
35		The following assert is written to the log file if a change is made to the conference layout while participants are disconnecting. BridgePartyVideoOut.cpp, Line:1458, Code:1701.; DEBUG-ASSERT:	12033	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
36	General	RMX 2000 string appears instead of RMX 4000 in the dialog box of error message when trying to export empty address book.	12056	
37		After upgrading to Version 5.0 (from 4.0.3, 4.1.0, 4.1.1), occasionally, the soft reset fails.	12100	1. First try to reset from the SHM if possible. 2. Otherwise hard reset the system.
38		While receiving a Re-invite from a remote endpoint, with lower H.264 parameters than the current transmission mode, only Flow Control is executed instead of Full Change mode.	12136	
39		When trying to connect an endpoint after hot swapping an RTM ISDN card the endpoint may not connect and the following disconnection description is displayed: Internal Problem - 65022.	12155	
40		Dial-out prefixes are not sortable in the *ISDN Services* dialog box.	12173	
41		When running 10 conferences at a line rate of 768Kbps and changing the layout for H.323 & SIP participants, when terminating the conference an assert may appear.	12181	
42		RMX Menu > Help > About RMX contains no information.	12235	
43		Endpoints are disconnected after extended time period (8 hrs +) under load. Error message is displayed: “Unit not responding”.	12240	
44		Sometimes, after 8 hours or more of conferencing at line rates of 4Mbps in a highly loaded MCU, the video processing unit fails.	12241	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
45	General	In a conference where the participant becomes the chairperson and then switches between a secure or unsecure conference using DTMF (*71/ #71) codes, the chairperson hears a distorted message.	12245	
46		After creating a new gateway, using the Japanese RMX Web Client, the pop-up message has the wrong description.	12425	
47		In the Japanese RMX Web Client, the New Profile > Advanced tab needs additional menu translations.	12426	
48		In English and Japanese RMX Web Clients, the “Terminal Viewer” fails to open. When using Administration > Turn On SSH and Administration > Tools > Terminal commands, a message, “Failed to open Terminal Viewer “is displayed.	12449	Make sure that SSH is Turned on.
49		When the RMX is set to *Flexible Allocation Mode* and more than 14 endpoints are connected to a single MPM+80 card in line rates above 2Mbps, video artifacts may appear.	10100, 11422	Change the resource *Allocation Mode* to ***Fixed*** *Mode*.
50		After software upgrade, it is necessary to close and reopen Internet explorer.	11883/ 11257	
51		Rarely, during a web browser connection, a Microsoft .NET framework message may appear.	11926/ 12001	Reopen the internet explorer.
52	H.323	The following asserts may appear when an H.323 participant connects to a 2 Mb Continuous Presence conference: File:AuditorApi.cpp, Line:112, Code:1.; ASSERT:Audit_free_Data_is_too_long_20882,_max_is_20480data_size_is_:_20882	11810	
53	Hardware	In D-type chassis, when hot-swapping an MPM card, unit failure may occur.	9571	Reset the MCU.

Table 13 Version 5.1.0.G System Limitations

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
54	HD	In HD Video Switching conferences, Tandberg endpoints may connect as Secondary when HD frame rate capabilities are less than 7.5 frames per second.	3089	Use HDCP.
55		In a H.323 conference with a line rate of 1920 Kbps and the Video set to Sharpness & Auto Layout, Aethra X7 endpoints receive 1024x576 instead of 720p HD.	11429	
56	Interoperability	Faulty connection status is indicated when the RSS 2000 recording link is the only participant in a conference and its video stream is not synchronized.	3977	The video stream is synchronized when the first participant connects to the conference.
57		HDX/VSX endpoints cannot connect directly to conferences while registered with Cisco Gatekeeper using the IP##NID string.	4652	Connect directly using the MCU IP Address via the Transit Entry Queue.
58		Sony PCS G70 (v2.61) and Sony PCS-1(v3.41) endpoints cannot connect to conferences using SIP connections.	6902	Force the endpoints to connect using H.323 connection.
59		The video of Sony G70 endpoint that is connected to a conference over ISDN at line rate of 128Kbps freezes when receiving Content from an HDX endpoint.	8605	
60		Radvision ECS Gatekeeper set to Routed Mode is not forwarding the LPR parameters as required, causing HDX calls with LPR enabled to connect with no video.	9015	
61		HDX8000 (Release - 2.0.3.1-2729) and VSX3000 (9.0.1- 18.07.2008) endpoints connect at a higher line rate than the conference line rate.	9425	
62		When switching Content sending from an HDX9004 to Aethra X7 and back, Content is not received by Aethra X7.	9677	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
63	Interoperability	When dialing out to VSX6000A SIP endpoint from a CP conference at line rate of 1920Kbps, it connects as Secondary.	9816	
64		HDX endpoints may experience packet loss when the HDX endpoint's LAN Speed is configured to 100MB.	9830	Set the endpoint *LAN Speed* and *Duplex Mode* to Auto.
65		When dialing out to a Tandberg MXP ISDN endpoint, the IVR slide is not displayed, although the IVR message is played.	9909	
66		When sending content from CMAD in a 384Kbps call, changes in the video image are observed.	9928	
67		An HDX 2.5.0.2-3395 endpoint cannot control a Sony XG80 endpoint using FECC.	10162	
68		VSX6000/VSX3000 endpoints receive incorrect protocol and format in a encrypted conference with LPR enabled.	10880	
69		In a ISDN dial-in conference with a line rate of 384 Kbps, ISDN Tandberg MXP endpoints cannot view content.	10989	
70		During H.320 calls, Lip Sync issues occur when content is being sent.	11341	
71		In a H.323 conference that has a line rate of 1920 Kbps and is set to Auto Layout, Tandberg 1700 and Edge95 MXP endpoints receive 1024x576 instead of 720p HD format.	11406	
72		In a H.323 CP Conference with the Video Quality set to Sharpness, VSX6000 and V500 endpoints encounter video stills.	11412	
73		Sony PCS-XG80 endpoints are unable to send H.239 Content in H.323 encrypted calls on the RMX.	11421	

Table 13 Version 5.1.0.G System Limitations

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
74	Interoperability	When Tandberg MXP sends Content using H.323, ISDN endpoints cannot view Content.	11425	
75		In a H.323 conference with a line rate of 128 Kbps that includes content, Lifesize ISDN endpoints cannot view the Content.	11463	
76		The RMX does not open the audio channel when connecting a DSTK60 endpoint in a conference with a line rate of 384 Kbps.	11464	
77		Legacy endpoints occasionally cannot switch from 1x1 to 7+1 video layouts when Content is started.	11480, 11492, 11563	
78		In a conference with a line rate of 384 Kbps, when and HDX 8006 endpoint that sends content is moved to another conference, content is still viewed for a number of seconds on the HDX.	11489	
79		When endpoints connect to a conference running on the RMX through the DMA, the endpoints will see full screen (1x1) layout and not the conference layout.	11508	
80		In a conference with a line rate of 1920 Kbps, when the RMX dials-out to a Sony XG80, the HD video may display fragmentation or artifacts.	11512	
81		In a conference started using the default factory profile, when connecting to the conference with a MOC Client or HDX SIP endpoint, there is no indication on the RMX if audio is muted or unmuted.	11523	
82		H.239 content sometimes cannot be seen on PVX endpoint (Version 8.5.0.4) when connected to the RMX, using H.264 protocol. The PVX endpoint is shown as 'connected with problem'.	11724	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
83	Interoperability	In a 6 Mb, Video Switched conference, an HDX endpoint that declares 2 Mb capability may only connect at 896 Kbps after 30 seconds.	11767	
84		When Tandberg C20 endpoint sends Content, the far end indicates that Content is being received but received Content is black.	11798	
85		Sony XG80 endpoint cannot send Content in H.323 in 384 Kbps call.	11830	
86		A PVX endpoint sometimes cannot receive H.239 content from an RMX 2000.	11882	
87		In a 4 Mb RPX conference with LPR enabled, video-out bit rate that decreases to 128 Kbps due to packet loss and does not increase.	11920	
88		In a CIF conference with a 384 Kbps line rate with AES, LPR and Video Clarity enabled, HDX IP endpoints connect to conference using a 4CIF resolution.	11963	
89		In a conference with AES, LPR and Video Clarity enabled, H.320 Tandberg MXP endpoints connect in a 960x720 resolution, while identical H.323 MXP endpoints connect in 720p.	12177	
90		In a conference with AES, LPR and Video Clarity enabled, H.320 HDX8006/HDX9004 endpoints only send Content in H.263.	12178	
91		Tandberg MXP endpoint receives ghosted video from HDX9004 endpoint during H.323 conference.	12266	
92		IVR welcome message is not clear on an Ipower v6.2.0.1208 endpoint connecting to RMX with Siren 14 or G722.1.	12273	
93		DST K60 endpoint receives tiled video from HDX9004 endpoint during H.323 conference.	12355	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
94	Interoperability	Tandberg C20 endpoint display fast updates in HD1080p conferences.	12369	
95		Tandberg 6000 E and B series H.320 endpoints do not connect to conference when encryption is turned on.	12372	
96		HDX endpoint connected via H.320 does not receive Content from Tandberg MXP endpoint connected via H.323.	12373	
97		VSX5000 endpoint freezes followed by disconnection of all VSX endpoints.	12559	
98		A black screen may appear on HDX8000 HD Hardware Version B endpoints when the conference line rate is set in the range of 256-768 Kbps. The Hardware version can be found on the HDX endpoint's *System Information* page.	10849 (i)	(1) Upgrade to HDX software Version 2.5.0.5 (2) Use conference line rates below 256 or above 768 Kbps. (3) Disable the IVR Welcome slide and avoid using a 1x1 Video Layout.
99		A black screen may appear on HDX SD endpoints using the PAL mode when the conference line rate is set above 128 Kbps.	10849 (ii)	
100		H.323 link is connected as secondary when cascading with Tandberg MPS at 768Kbps, in both Video Switching and CP conferences.	7597/ 7598	
101		Tandberg C20 and C90 SIP endpoints connect as Audio Only in 4 mbps, VSW, HD720p, (Video Quality=Sharpness) conference at line rates above 1920 kbps on RMX2000 running V5.1.0.25_P3	15721	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
102	Interoperability	Tandberg C20 endpoint stops receiving video when the HDX8006 sends content during 6 mbps HD1080p VSW sharpness, encrypted conference on RMX2000 in running V5.1.0.25_P3.	15719	
103		Video freezes throughout the duration of conference on Tandberg 6000 MXP, H.320 endpoint during 384 kbps, CP, Auto layout, encrypted, motion conference on RMX2000 running V5.1.0.25_P3.	15706	
104		Tandberg 6000 MXP H.320 endpoint receives poor quality content from Tandberg Edge95 MXP H.323 endpoint during 384 kbps, CP, Auto layout, encrypted, motion conference on RMX2000 running V5.1.0.25_P3.	15704	
105		HDX8006 endpoint sometimes displays black video when connected via H.320 to 4 mbps, HD720p, sharpness, encrypted call.	15679	
106		Tandberg MXP F8.2 endpoint's video is not received by conference and its status is displayed as: Connected with problem, when HDX8006 H.320 endpoint sends content in 4 mbps, sharpness, encrypted call on RMX2000 running v5.1.0.25_P3.	15678	
107		Tandberg C20 endpoint is unable to send content successfully to Tandberg Edge95 MXP endpoint in 768 kbps CP, auto layout sharpness, encrypted conference with content set for up to H.264 if its content is set for H.263 on RMX2000 running V5.1.0.25_P3.	15676	
108		Tandberg MXP F8.2 endpoint freezes with Welcome Slide displayed when RMX running v5.1.0.25_P3 dials 1920 kbps, sharpness call to Tandberg 1700 MXP.	15677	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
109	IP	Static Routes table in IP Network Service does not function.	7734	
110		When changing the new system mode from IPv4 to or from IPv6 Auto/Manual, the system does not reset.	12053	
111	ISDN	The following assert occurs when encrypted ISDN endpoints connected with a “Connected with Problem” status. Segment.cpp, Line:650, Code:127.; ASSERT:	11872	
112		ISDN EP does not display IVR slide.	11908	
113		When ISDN participants connect to a conference with line rate 384kbs, multiple asserts appear in the log file.	12007	
114		Occasionally, an ISDN participant fails to connect to the conference due to the following error - “MCU internal problem - 50020".	12011	
115		Removing the main or backup PRI clock source causes disconnection of all connected IP and ISDN participants.	12370	
116	ISDN Encryption	In a conference with a 384 Kbps line rate, an H.320 encrypted participant cannot connect and an assert appears.	12034	
117	ISDN/PSTN	When a busy signal is returned by a PSTN dial-out participant, the RMX does not redial but disconnects the participant with *“party hung-up-0*” status.	4405	
118	IVR	Customized CIF slide is not displayed on the HDX screen when connecting to a 1080p High Definition Video Switching conference.	10054	
119		In a SIP CP conference with a line rate of 2 Mb, HDX 8006 endpoints cannot view the IVR slide.	10824	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
120	IVR	After upgrading the RMX to software version that includes the gateway the maximum number of IVR services was reached 40 in RMX 2000 and 80 in RMX 4000), the default Gateway IVR Service is not created.	11531	
121		Welcome slide is not displayed when a dial-out SIP endpoint connects at a line rate of 768 Kbps, using H261 video protocol.	11712	
122		In the conference with a 2Mb line rate when a single participant enters the conference the participant does not hear music.	12116	
123		When DTMF codes have been entered by the participants, the volume of the IVR Message may be suppressed.	9191 9809 9834	
124	IVR - RMX 4000	On the RMX 4000, when dialing from ISDN endpoint to GW, the IVR Welcome message is cut off.	12283	
125		On the RMX 4000, when dialing from ISDN endpoint to GW, video artifacts appear in the IVR slide.	12284	
126		On the RMX 4000 that was upgraded from an earlier version, when connecting participant to a conf, RMX2000 slides are displayed instead of RMX 4000.	13358	Perform *Restore Factory Defaults* and then *Restore System Configuration* without the old IVR Services.
127	LPR	When an H.323 HDX endpoint sends Content, the endpoint disables the LPR.	10104	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
128	LPR	Reduced video quality may be observed when using LPR with HD720p. When packet loss is detected by the LPR mechanism, the LPR lowers the call bit rate to keep the video quality of the call. When excessive packet loss exists, the call rate may drop down to 128K, using HD 720p under these conditions will result in a reduced video image quality.	11020	
129	Multilingual	The Display Name of undefined dial-in participant using HDX and VSX 7000 endpoints is displayed in English in the *RMX Web Client*.	5151	
130		Multilingual Settings are not reflected on the Shelf Management login page and the multilingual flags appear in the Shelf Manager window even when they have not been selected in the Multilingual Settings pane.	5310	
131	RMX Web Client	When connecting directly to the Shelf Manager and selecting Diagnostic Mode the CNTL module does not enter the diagnostic mode and stays “Normal”.	7557	Reset the MCU and then switch to Diagnostic Mode
132	Security	If an RMX, operating in Secure Communication Mode, is downgraded to a version that does not support Secure Communication Mode (V2.0, V1.1), all connectivity to the RMX is lost.	8259	Cancel the Secure Mode before downgrading
133		DOS vulnerability exists in NTP Daemon. Response to mode 7 error packets with its own mode 7 error packets could be exploited by attacker sending a mode 7 error response with a spoofed IP header, setting the source and destination IP addresses to the IP address of the target. NTP would respond to itself endlessly, consuming excessive amounts of CPU resources, resulting in a denial of service.	16228	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
134	Security	Access is possible via Keyboard and VGA ports while system is in JITC mode In JITC Mode.	15915	
135	SIP	SIP participants cannot connect to a conference when the conference name contains blank spaces.	3276	
136		With SIP defined and undefined dial-in participants you cannot change the layout type from “conference layout” to “personal layout”.	12006	
137	Software	When trying to restore last version, after upgrading from Version 3 to Version 4, the RMX prompts for an activation key.	9228	
138	Software Version	When downgrading from Version 4.0 to Version 3.0 the MPM card does not revert to normal.	9565	Reset the MCU
139		When upgrading from Version 2.0.2 to Version 4.1, and then Restoring the Factory Defaults, during system restart sometimes MPL failure is encountered.	9740	Turn the MCU off and then turn it on (“hardware” reset).
140		Active alarm: SystemMonitoring FAILED to start during Startup !!!, is displayed after Restore to Factory Default is performed on RMX4000 with 2*MPM+80 cards. Hard Reset solves this issue.	16420	Hard Reset the RMX.
141		.Net Exception occurs when connecting participant to conference on RMX4000 with two Networks configured in JITC mode.	16273	
142		Core Dump of Apache Module occurs on RMX running V5.1.0.27 in JITC Mode.	15874	
143		Restore to factory default from USB with the lan.cfg file causes RMX to enter restart loop.	15043	
144	Upgrade Process	Upgrade of RMX2000/4000 from V5.1.0.34 to V7.0.0.139 fails with message: Installation of MCU version failed.	16869	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
145	Video	In a 4Mb conference set to Sharpness and the IVR Welcome Message enable video appears in a 4x3 format. Disable IVR Welcome message and the video appears in 6x9 format.	10239	
146		When the Closed Caption text is very long the text is split and may be displayed incorrectly.	11123	
147		When the video from an endpoint is blocked, inconsistent video resolution settings are implemented.	11351	
148		Legacy endpoints receive Content in 1+7 layout with black stripes on the sides (for aspect ratio fitting), selecting a different layout using Click&View (**) causes the black stripes to disappear.	11382	
149		When the VVX1500 is forced to H.263 in SIP calls, the endpoint cannot receive video from the RMX.	11541	Don't force the VVX1500 to H.263.
150		In a 2 Mb Video Switched conference with 10 or more H.323 endpoints connected, random video refreshes may occur.	11843	
151		In a conference with a 384 Kbps line rate with AES and LPR enabled, calls connect using the H.263 instead of the H.264 video protocol.	11965	
152		In a conference running at line rate of 4Mb and resolution of HD1080p, some HDX endpoints (H.323 & SIP) encounter video problems due to a DSP failure.	12217	
153	Web Client	Sometimes when installing the *RMX Web Client*, Windows Explorer >Internet Options> Security Settings must be set to *Medium* or less.	2473	
154		Occasionally, during an ongoing conference, when selecting the Hardware Monitor menu the message "No connection with Switch" appears.	9829	

Table 13 *Version 5.1.0.G System Limitations*

No.	Category	Description	ID/ VNGR#	Workaround/ Remarks
155	Web Client	In the RMX Web Client, the main window opens up as full screen and cannot be resized.	12172	
156		In the RMX Web Client when viewing the *Conference Properties - General*, the keyboard *Tab* button does not move the cursor to the next field.	12176	Keep pressing on the Tab button.
157		When upgrading the RMX Web Client with software changes, Internet Explorer needs to be closed and opened before the upgrade can take place.	12257	